

Installationshandbuch

McAfee ePolicy Orchestrator 5.0.0 – Software

Inhaltsverzeichnis

Einleitung

Inhalt

Informationen zu diesem Handbuch

In diesem Abschnitt werden die Zielgruppe des Handbuchs, die verwendeten typografischen Konventionen und Symbole sowie die Gliederung des Handbuchs beschrieben.

Zielgruppe

Die Dokumentation von McAfee wird inhaltlich sorgfältig auf die Zielgruppe abgestimmt.

Die Informationen in diesem Handbuch richten sich in erster Linie an:

- **Administratoren** – Personen, die das Sicherheitsprogramm eines Unternehmens implementieren und umsetzen.
- **Benutzer** – Personen, die den Computer verwenden, auf dem die Software ausgeführt wird, und die auf einige oder alle Funktionen zugreifen können.
- **Prüfer** – Personen, die das Produkt bewerten.

Konventionen

In diesem Handbuch werden folgende typografische Konventionen und Symbole verwendet.

Buchtitel, *Begriff*, *Hervorhebung*	Titel eines Buchs, Kapitels oder Themas; ein neuer Begriff; eine Hervorhebung.
Fett	Text, der stark hervorgehoben wird.
`Benutzereingabe, Code, Meldung`	Befehle oder andere Texte, die vom Benutzer eingegeben werden; ein Code-Beispiel; eine angezeigte Meldung.
Benutzeroberflächentext	Wörter aus der Benutzeroberfläche des Produkts, z. B. Optionen, Menüs, Schaltflächen und Dialogfelder.
Hypertext-Blau	Ein Link auf ein Thema oder eine externe Website.
	Hinweis: Zusätzliche Informationen, beispielsweise eine alternative Methode für den Zugriff auf eine Option.
	**Tipp:** Vorschläge und Empfehlungen.



Wichtig/Vorsicht: Wichtige Ratschläge zum Schutz Ihres Computersystems, der Software-Installation, des Netzwerks, Ihres Unternehmens oder Ihrer Daten.



Warnung: Wichtige Ratschläge, um körperliche Verletzungen bei der Nutzung eines Hardware-Produkts zu vermeiden.

Quellen für Produktinformationen

McAfee stellt Ihnen die Informationen zur Verfügung, die Sie in den einzelnen Phasen der Produktimplementierung benötigen – von der Installation bis hin zur täglichen Nutzung und Fehlerbehebung. Nach der Produktveröffentlichung erhalten Sie Informationen zu diesem Produkt online in der KnowledgeBase von McAfee.

Vorgehensweise

1 Wechseln Sie zum McAfee Technical Support ServicePortal unter http://mysupport.mcafee.com.

2 Greifen Sie unter **Self Service** (Online-Support) auf die erforderlichen Informationen zu:

Zugriff auf	Vorgehensweise
Benutzerdokumentation	1 Klicken Sie auf **Product Documentation** (Produktdokumentation). 2 Wählen Sie ein Produkt und dann eine Version aus. 3 Wählen Sie ein Produktdokument aus.
KnowledgeBase	• Klicken Sie auf **Search the KnowledgeBase** (KnowledgeBase durchsuchen), um Antworten auf Ihre produktbezogenen Fragen zu erhalten. • Klicken Sie auf **Browse the KnowledgeBase** (KnowledgeBase durchblättern), um Artikel nach Produkt und Version aufzulisten.

1 Anforderungen und Empfehlungen für die Installation

Zum Ausführen von McAfee® ePolicy Orchestrator® 5.0 muss eine Umgebung über bestimmte Hard- und Software verfügen. Lesen Sie diese Anforderungen und Empfehlungen vor Beginn der Installation von McAfee ePO™ sorgfältig durch, um sicherzustellen, dass Ihre Installation erfolgreich verläuft.

Inhalt

Anforderungen und Empfehlungen für Hardware

Vor der Installation von ePolicy Orchestrator müssen Sie sicherstellen, dass Ihre Umgebung die folgenden Anforderungen und Empfehlungen erfüllt.

Komponente	Anforderungen und Empfehlungen
Dedizierter Server	Wenn mehr als 250 Systeme verwaltet werden sollen, wird der Einsatz eines dedizierten Servers empfohlen.
Domänen-Controller	Der Server muss in einem Vertrauensverhältnis zum Domänen-Controller im Netzwerk stehen. Entsprechende Anweisungen finden Sie in der Dokumentation des Microsoft-Produkts.
Dateisystem	Empfohlen wird eine Partition mit dem NT-Dateisystem (NTFS).
Verfügbarer Speicherplatz	5 GB – Empfohlener Mindestspeicher
IP-Adresse	Für ePolicy Orchestrator-Server werden statische IP-Adressen empfohlen. ePolicy Orchestrator unterstützt sowohl IPv4- als auch IPv6-Netzwerke.
Arbeitsspeicher	Mindestens 4 GB verfügbarer Arbeitsspeicher empfohlen

Komponente	Anforderungen und Empfehlungen
Netzwerkkarte	100 MBit (oder schneller) Bei Verwendung eines Servers mit mehreren IP-Adressen nutzt ePolicy Orchestrator die erste identifizierte IP-Adresse. Wenn Sie für die Kommunikation zwischen Agent und Server weitere IP-Adressen verwenden möchten, sollten Sie für jede IP-Adresse zusätzliche Agentensteuerungsgruppen erstellen. Ausführliche Informationen zum Einrichten von Agentensteuerungsgruppen finden Sie unter *Arbeiten mit Agentensteuerungen* im *Produkthandbuch von ePolicy Orchestrator* oder in der Hilfe.
Ports	Es wird empfohlen, den Port 8443 für die HTTPS-Kommunikation zu vermeiden. Obwohl dies der Standardport ist, wird er auch von vielen Web-basierten Aktivitäten als primärer Port genutzt und ist deshalb ein Ziel für böswillige Angriffe. Daher wird dieser Port oft vom Systemadministrator deaktiviert, wenn eine Sicherheitsverletzung oder ein Malware-Befall auftritt. Stellen Sie sicher, dass die gewählten Ports nicht bereits auf dem Server-System verwendet werden. Informieren Sie das Netzwerkpersonal über die Ports, die für die HTTP- und HTTPS-Kommunikation genutzt werden sollen. Die Installation der Software auf einem Domänen-Controller wird unterstützt, aber nicht empfohlen.
Prozessor	• 64-Bit Intel Pentium D (oder höher) • 2,66 GHz (oder schneller)

Anforderungen und Empfehlungen für Software

Vor dem Installieren von ePolicy Orchestrator müssen Sie sicherstellen, dass auf Ihrem Server-System die erforderliche und empfohlene Software installiert ist.

Software	Anforderungen und Empfehlungen
Microsoft .NET Framework 2.0 oder höher	Erforderlich – Diese Software müssen Sie manuell herunterladen und installieren. Diese Software ist erforderlich, wenn Sie eine Installationsoption auswählen, bei der SQL Server Express 2008 aus dem Lieferumfang dieser ePolicy Orchestrator-Software automatisch installiert wird. Wenn diese Software fehlt, müssen Sie das Setup beenden und die Software manuell installieren, bevor Sie fortfahren können.
Microsoft-Updates	Empfohlen – Stellen Sie sicher, dass Ihre Microsoft-Software mit den aktuellen Updates ausgeführt wird. Deaktivieren Sie Windows-Updates, bevor Sie mit dem Installieren oder Aktualisieren Ihrer Software beginnen.
Microsoft Visual C++ 2005 SP1 Redistributable	Erforderlich – Wird automatisch installiert.
Microsoft Visual C++ 2008 Redistributable Package (x86)	Erforderlich – Wird automatisch installiert.
MSXML 6.0	Erforderlich – Wird automatisch installiert.

Software	Anforderungen und Empfehlungen
Sicherheits-Software	Empfohlen. • Installieren und/oder aktualisieren Sie die Antiviren-Software auf dem Server, und führen Sie einen Scan durch. • Installieren und/oder aktualisieren Sie die Firewall-Software auf dem Server. Wenn auf dem System, auf dem Sie ePolicy Orchestrator installieren möchten, McAfee VirusScan® Enterprise 8.5i oder 8.7i ausgeführt wird, müssen Sie sicherstellen, dass die VSE-Zugriffsschutzregeln während des Installationsvorgangs deaktiviert sind, da die Installation andernfalls fehlschlägt.
Unterstützter Browser	Empfohlen – Auch wenn für die Installation nicht benötigt, erfordert ePolicy Orchestrator die Verwendung eines unterstützten Browsers. Sie müssen einen unterstützten Browser manuell herunterladen und installieren. Weitere Informationen dazu finden Sie unter *Unterstützte Internet-Browser*.
Unterstützte SQL Server-Version	Erforderlich – Wenn noch keine unterstützte Version von SQL Server installiert ist, können Sie festlegen, dass SQL Server 2008 Express automatisch installiert werden soll.

Unterstützte Betriebssysteme

ePolicy Orchestrator kann auf beliebigen unterstützten Microsoft Windows Server-Betriebssystemen installiert werden.

Unterstützte Server-Betriebssysteme

Für die Software ist eines der folgenden unterstützten 64-Bit-Server-Betriebssysteme erforderlich.

Unterstütztes Betriebssystem	64-Bit
Windows Server 2008 (mit Service Pack 2 oder höher)	X
Windows Server 2012	X

Nicht unterstützte Betriebssysteme

ePolicy Orchestrator kann testweise auf den nicht unterstützten 64-Bit-Versionen von Windows 7 oder Windows 8 ausgeführt werden.



Die Installation von ePolicy Orchestrator auf Windows 7 oder Windows 8 dient nur zu **Testzwecken**. McAfee stellt dafür keine Unterstützung bereit.

Sprache des Betriebssystems

ePolicy Orchestrator läuft auf allen unterstützten Betriebssystemen ungeachtet der im jeweiligen Betriebssystem eingestellten Sprache.

Die Benutzeroberfläche von ePolicy Orchestrator wurde in die nachfolgend aufgeführten Sprachen übersetzt. Wenn die Software unter einem Betriebssystem installiert wird, in dem eine andere Sprache als hier aufgeführt eingestellt ist, wird die Benutzeroberfläche auf Englisch angezeigt.

- Chinesisch (Vereinfacht)
- Chinesisch (Traditionell)
- Dänisch
- Niederländisch
- Englisch
- Finnisch
- Französisch (Standard)
- Deutsch (Standard)
- Italienisch
- Japanisch
- Koreanisch
- Norwegisch
- Portugiesisch (Brasilien)
- Portugiesisch (Iberisch)
- Russisch
- Spanisch
- Schwedisch
- Türkisch

Unterstützte Software für die virtuelle Infrastruktur

ePolicy Orchestrator unterstützt die Verwendung von Software für verschiedene Typen von virtueller Infrastruktur.

Unterstützte Software für die virtuelle Infrastruktur:

- Microsoft Hyper-V Server 2008 R2
- Microsoft Hyper-V Server 2012
- VMware ESX 5.0
- VMware ESX 5.1
- XenServer 6

Unterstützte SQL Server-Versionen

Für ePolicy Orchestrator ist die Nutzung einer unterstützten SQL Server-Installation erforderlich.

Der Installations-Assistent ermittelt, ob auf dem Server-System, auf dem die Software installiert werden soll, eine unterstützte SQL Server-Version vorhanden ist. Wenn keine SQL Server-Installation vorhanden ist, werden Sie vom Assistenten aufgefordert, Microsoft SQL Server 2008 Express lokal zu installieren oder einen vorhandenen SQL-Server auszuwählen.

Version	Edition
Microsoft SQL Server 2008 R2 32-Bit und 64-Bit (mit Service Pack 1 oder höher)	• Enterprise Edition • Express Edition • Standard Edition • Workgroup Edition
Microsoft SQL Server 2012 (32- und 64-Bit)	• Enterprise Edition • Express Edition • Standard Edition • Business Intelligence Edition

Erforderliche Konfigurationseinstellungen in SQL Server

Für ePolicy Orchestrator sind einige spezielle Konfigurationseinstellungen in SQL Server erforderlich. Informationen zur Arbeit mit diesen Einstellungen finden Sie in der Dokumentation Ihres SQL-Servers.

Konfiguration	Details
Geschachtelte Trigger	Die Option **Geschachtelte Trigger** von SQL Server muss aktiviert sein.
Datenbanksortierung	Von ePolicy Orchestrator wird nur die folgende Standard-Datenbanksortierung für amerikanisches Englisch unterstützt: SQL_Latin1_General_Cp1_CI_AS.
Wartungseinstellungen	Es wird empfohlen, bestimmte Wartungseinstellungen an ePolicy Orchestrator-Datenbanken vorzunehmen. Weitere Informationen hierzu finden Sie im *Produkthandbuch von McAfee ePolicy Orchestrator* oder in der Hilfe.

Unterstützte Internet-Browser

Für ePolicy Orchestrator ist einer der folgenden unterstützten Internet-Browser erforderlich.

- Internet Explorer 8.0 und höher (mit vollständiger Unterstützung des Kompatibilitätsmodus)
- Firefox 10.0 und höher
- Chrome 17 und höher
- Safari 6.0 und höher (MAC OS X, Windows wird nicht unterstützt)

Verwenden von verstärkter Sicherheit in Internet Explorer

Wenn Sie Internet Explorer mit verstärkter Sicherheit verwenden, müssen Sie die ePolicy Orchestrator-Server-Adresse (im Format `https://<Server-Name>`) zur Liste der vertrauenswürdigen Sites in Internet Explorer hinzufügen. Andernfalls wird bei dem Versuch, sich beim ePolicy Orchestrator-Server anzumelden, die Fehlermeldung Sie müssen JavaScript aktivieren, um dieses Produkt verwenden zu können angezeigt.

Server-Anforderungen für Agentensteuerungen

ePolicy Orchestrator-Agentensteuerungen können auf beliebigen unterstützten Microsoft Windows Server-Betriebssystemen installiert werden.

Für Agentensteuerungen ist eines der folgenden Server-Betriebssysteme erforderlich.

Betriebssystem	32-Bit	64-Bit
Windows Server 2008	X	X
Windows Server 2012	X	X

Vorbereiten auf die Installation

Vor Beginn der Installation von ePolicy Orchestrator müssen Sie alle benötigten Informationen sowie deren Speicherort kennen und wissen, welche Schritte durchzuführen sind.



Lesen Sie sich die folgenden Informationen sorgfältig durch, bevor Sie mit der Installation beginnen.

Lesen, verstehen und befolgen Sie unbedingt die im Kapitel *Anforderungen und Empfehlungen für die Installation* aufgeführten Punkte, bevor Sie mit der Installation beginnen.

Halten Sie während der Installation die folgenden Informationen bereit:

- McAfee-Produktlizenzschlüssel (beim Installieren einer Testversion nicht erforderlich).
- Für die Microsoft SQL-Authentifizierung sind Anmeldeinformationen eines der folgenden Typen erforderlich:
  - Anmeldeinformationen für die Windows-Authentifizierung – Anmeldeinformationen für ein Domänenadministrator-Benutzerkonto.
  - Anmeldeinformationen für die SQL-Authentifizierung – Weitere Informationen zu erforderlichen SQL Server-Berechtigungen finden Sie unter *Informationen zu den für die Installation erforderlichen SQL Server-Rollen*.
- Einen Zielordner für die ePolicy Orchestrator-Installation (bei benutzerdefinierten und Cluster-Installationen erforderlich).
- Einen unterstützten SQL Server.
- Bei Verwendung einer neuen, manuell installierten oder einer bereits vorhandenen Instanz von SQL Server müssen Sie während des Installationsvorgangs möglicherweise (je nach Konfiguration) die folgenden Informationen auf der Seite **Datenbankinformationen** angeben:
  - Den Namen des SQL-Servers. Dieser Name sollte zusammen mit dem SQL-Server-Namen oder dem SQL-Server-Namen *und* dem Instanznamen angegeben werden.
  - Die vom SQL-Server verwendete dynamische Portnummer.
- Bei einer Wiederherstellung des ePolicy Orchestrator-Servers müssen folgende Bedingungen erfüllt sein:
  - Sie müssen zuvor die SQL Server-Datenbank mithilfe eines der Microsoft SQL-Wiederherstellungsprozesse wiederhergestellt haben. Ausführliche Informationen dazu finden Sie im *Produkthandbuch von McAfee ePolicy Orchestrator*.
  - Sie müssen die Passphrase für die Schlüsselspeicherverschlüsselung kennen, mit der die Datensätze aus dem Snapshot für die Wiederherstellung nach einem Systemausfall verschlüsselt wurden. Diese Passphrase dient zum Entschlüsseln der in den SQL-Snapshot-Datensätzen gespeicherten vertraulichen ePolicy Orchestrator-Informationen.

Informationen zu der in diesem Handbuch dokumentierten SQL Server-Installation

Für ePolicy Orchestrator ist die Nutzung einer unterstützten SQL Server-Installation erforderlich. Das einzige in dieser Anleitung detailliert beschriebene Installationsszenario ist eine Erstinstallation von SQL Server 2008 Express.
In diesem Szenario werden vom InstallShield-Assistenten sowohl die ePolicy Orchestrator-Software als auch die SQL Server-Software auf demselben System installiert. Wenn SQL Server auf einem anderen als dem McAfee ePO-Server installiert werden soll, müssen Sie die Installation manuell vornehmen. Weitere Informationen über das Installieren einer anderen unterstützten SQL Server-Version finden Sie in der Dokumentation der SQL Server-Software.



Bei einer Cluster-Installation müssen Sie eine manuell installierte SQL Server-Installation verwenden, die sich auf einem anderen System befindet als auf dem, auf dem Sie ePolicy Orchestrator installieren.

Andere relevante SQL Server-Installationen und -aktualisierungen

In der Microsoft-Dokumentation finden Sie Informationen zu den folgenden Installationsszenarien:

- Installieren von SQL Server 2008 oder SQL Server 2012
- Aktualisieren von SQL Server 2005 auf SQL Server 2008 oder SQL Server 2012
- Aktualisieren von SQL Server 2005 Express auf SQL Server 2008 Express oder SQL Server 2012 Express

Informationen zu den für die Installation erforderlichen SQL Server-Rollen

Wenn Sie für Ihre ePolicy Orchestrator-Software eine vorhandene Instanz von SQL Server verwenden möchten, sind für eine erfolgreiche Installation bestimmte SQL Server-Rollen erforderlich.

Wenn Sie eine vorhandene SQL Server-Installation verwenden möchten oder eine neue SQL Server-Instanz manuell installieren, müssen Sie während der Installation von ePolicy Orchestrator Anmeldeinformationen angeben. Das Benutzerkonto, dem diese Anmeldeinformationen entweder für eine Windows- oder eine SQL-Authentifizierung zugewiesen sind, muss auf dem SQL-Ziel-Server über die Server-Rolle "dbcreator" verfügen. Diese Server-Rolle wird vom Setup-Programm benötigt, um während der Installation die erforderlichen ePolicy Orchestrator-Hauptdatenbankobjekte zu erstellen und auf dem SQL-Ziel-Server hinzuzufügen.

In der Standardeinstellung wird diesem Benutzerkonto, nachdem die Hauptdatenbank erstellt wurde, die Datenbankrolle "db_owner" für die ePolicy Orchestrator-Datenbank gewährt. Nach Abschluss der Installation kann die Server-Rolle "dbcreator" für dieses Benutzerkonto wieder gesperrt werden. Durch das Aufheben der Server-Rolle "dbcreator" wird das Konto auf die Berechtigungen eingeschränkt, über die die Datenbankrolle "db_owner" für die Hauptdatenbank verfügt.

Weitere Informationen zu den einzelnen standardmäßigen SQL-Datenbankrollen, die für einen ordnungsgemäßen Betrieb des ePolicy Orchestrator-Servers erforderlich sind, finden Sie im Produkthandbuch oder in der Hilfe. Eine vollständige Beschreibung der SQL Server-Rollen und -Berechtigungen finden Sie in der Produktdokumentation des unterstützten SQL Server-Produkts, das Sie verwenden.

Informationen zu HTTP-Port-Optionen

Die von ePolicy Orchestrator verwendeten Ports sind vorab festgelegt und werden in der Standardeinstellung vorgegeben. Die meisten Portangaben können nur während des Installationsvorgangs geändert werden.

In der folgenden Tabelle ist aufgeführt, welche Portzuweisungen Sie ändern können.

Port	Standardwert	Kann während der Installation geändert werden	Kann nach der Installation geändert werden
Port für Agent-zu-Server-Kommunikation	80	X	
Sicherer Port für Agent-zu-Server-Kommunikation	443	X	
Kommunikationsport für Agenten-Reaktivierung	8081	X	X
Kommunikationsport für Agenten-Übertragung	8082	X	X
Konsolen-Port zur Anwendungs-Server-Kommunikation	8443	X	
Port für authentifizierte Agent-zu-Server-Kommunikation	8444	X	
Port für Benachrichtigungen über Sicherheitsbedrohungen	8801		
TCP-Port für SQL-Server	1433	X	

Anforderungen an verteilte Repositories

Mithilfe von verteilten Repositories wird in Ihrer Umgebung der Zugriff auf wichtige, von Ihrem ePolicy Orchestrator-Server verwendete Inhalte ermöglicht. Ihre verteilten Repositories müssen die folgenden Mindestanforderungen erfüllen.

Komponente	Voraussetzungen
Verfügbarer Speicherplatz	Auf dem Laufwerk, auf dem sich das Repository befindet, sollten mindestens 400 MB (empfohlen werden 800 MB) frei sein. Wie viel Speicherplatz tatsächlich benötigt wird, hängt davon ab, welche Menge an Daten bereitgestellt werden soll. Die Speicherplatzanforderung für die verteilten Repositories auf Systemen, auf denen Agenten als SuperAgents gekennzeichnet sind, entspricht dem Speicherplatz, der für das Master-Repository verfügbar sein muss.
Arbeitsspeicher	Mindestens 256 MB.
Repository-Hosts	• HTTP-kompatible Server unter Microsoft Windows oder Linux • FTP-Server unter Windows, Linux oder Open Enterprise • UNC-Freigaben unter Windows, Linux, oder UNIX Samba • Systeme, auf denen ein SuperAgent installiert ist

Unterstützte und nicht unterstützte Produkte

Vor einer Installation oder Aktualisierung sollten Sie die Liste der von ePolicy Orchestrator unterstützten Produkte durchsehen.

Eine aktualisierte Liste mit unterstützten bzw. nicht unterstützten Produkten finden Sie in den folgenden KnowledgeBase-Artikeln:

- Von McAfee ePO 5.0 unterstützte Produkte – KB76736 (https://kc.mcafee.com/corporate/index?page=content&id=KB76736)
- Von McAfee ePO 5.0 nicht unterstützte Produkte – KB76737 (https://kc.mcafee.com/corporate/index?page=content&id=KB76737)
- Prüfliste mit bekannten Problemen bei der McAfee ePO 5.0-Installation bzw. dem Upgrade mithilfe eines Patches – KB76739 (https://kc.mcafee.com/corporate/index?page=content&id=KB76739)

2 Installieren von McAfee ePolicy Orchestrator

Sie können ePolicy Orchestrator entweder als erstmalige Neuinstallation oder als Wiederherstellungsinstallation installieren, bei der Ihr Microsoft SQL-Server bereits über eine ePolicy Orchestrator-Konfiguration aus einer vorherigen Installation verfügt.

Falls Sie eine Wiederherstellungsinstallation durchführen möchten, bei der Ihr Microsoft SQL-Server bereits über eine ePolicy Orchestrator-Konfiguration aus einer vorherigen Installation verfügt, finden Sie weitere Informationen dazu unter *Wiederherstellen von McAfee ePolicy Orchestrator*.

Inhalt

Optionen für eine Erstinstallation

Es gibt drei Optionen für eine Erstinstallation von ePolicy Orchestrator. Bei jeder dieser Optionen werden Sie vom InstallShield-Assistenten von ePolicy Orchestrator durch den Installationsvorgang geführt.

Welche Erstinstallationsoption für Ihre Umgebung geeignet ist, können Sie mithilfe der folgenden Tabelle bestimmen.

<table>
<tr><th>Installationsoption</th><th>Details</th></tr>
<tr><td>Express</td><td>Die direkteste Installationsweise. Wählen Sie diese Option, wenn Sie für Ihre Installation die Standardeinstellungen von McAfee übernehmen möchten.</td></tr>
<tr><td>Benutzerdefiniert</td><td>Hierbei können Sie die Installation nach Ihren Wünschen anpassen. Wählen Sie diese Option aus, wenn Sie die Details der Installation beeinflussen möchten, wie zum Beispiel:
• Den Zielordner, in dem die Software installiert werden soll (standardmäßig: <code>C:\Programme\McAfee\ePolicy Orchestrator\</code>).
• Die zu verwendenden Ports.
 Die Installation von SQL Server 2008 Express ist optional. Sie können auch eine andere unterstützte SQL Server-Version angeben, sofern SQL Server bereits vor Beginn der Installation von McAfee ePO installiert wurde.</td></tr>
<tr><td>Cluster</td><td>Führt eine Cluster-Installation durch. Wählen Sie diese Option aus, wenn Sie die Software in einer Cluster-Umgebung installieren möchten. Vor Beginn der Installation der Software müssen Sie Folgendes sicherstellen:
• Ihre MSCS-Umgebung (Microsoft Cluster Server) muss eingerichtet sein.
• Eine unterstützte SQL Server-Version muss in einem Speicherort installiert sein, auf den der Cluster zugreifen kann.</td></tr>
</table>

Wenn Sie eine frühere Version von McAfee ePolicy Orchestrator aktualisieren oder von einer Testversion migrieren, lesen Sie das Kapitel *Aktualisieren von McAfee ePolicy Orchestrator*.

Durchführen einer Express-Installation

Bei einer Express-Installation wird die ePolicy Orchestrator-Software in so wenigen Schritten wie möglich installiert, indem die Standardkonfiguration automatisch akzeptiert wird.

Bevor Sie beginnen

- Lesen, verstehen und befolgen Sie unbedingt die im Kapitel *Anforderungen und Empfehlungen für die Installation* aufgeführten Punkte.
- Aktualisieren Sie das System, das als Host für den ePolicy Orchestrator-Server dient, mit den aktuellen Microsoft-Sicherheits-Updates, und deaktivieren Sie dann Windows-Updates für die Dauer der Installation.



Es wird empfohlen, den gesamten Installationsvorgang zu überwachen. Möglicherweise müssen Sie das System neu starten.

Vorgehensweise

1. Melden Sie sich mit einem Konto, das über lokale Administratorrechte verfügt, bei dem Windows-Computer an, der als ePolicy Orchestrator-Server verwendet werden soll.
2. Bei Software, die Sie von der McAfee-Website heruntergeladen haben: Extrahieren Sie die Dateien in einen temporären Speicherort, und doppelklicken Sie auf **SETUP.EXE**. Die ausführbare Datei befindet sich in der heruntergeladenen ePolicy Orchestrator-Installationsdatei.

   Versuchen Sie nicht, die Datei `SETUP.EXE` auszuführen, bevor Sie den Inhalt der ZIP-Datei extrahiert haben.

   Der **McAfee ePolicy Orchestrator – InstallShield-Assistent** wird gestartet.

3 Klicken Sie auf eine der folgenden Optionen:
   - **Weiter**, wenn Sie eine normale ePolicy Orchestrator-Installation durchführen möchten.
   - **ePO aus einem vorhandenen Datenbank-Snapshot wiederherstellen** und **Weiter**, wenn Sie eine ePolicy Orchestrator-Wiederherstellungsinstallation durchführen möchten. Die ePolicy Orchestrator-Funktion "Snapshot für Wiederherstellung nach Systemausfall" ermöglicht nach einem Ausfall der Hardware, auf der sich der McAfee ePO-Server befindet, eine schnelle Wiederherstellung. Diese Funktion speichert die ePolicy Orchestrator-Konfiguration sowie Erweiterungen, Schlüssel und andere Informationen in Snapshot-Datensätzen in der ePolicy Orchestrator-Datenbank.



Bei einer Wiederherstellungsinstallation werden einige Erstinstallations-Dialogfelder zur Datenbankauswahl nicht angezeigt.

4 Wählen Sie im Schritt **Setup-Typ** die Option **Express** aus, und klicken Sie dann auf **Weiter**.

5 Wählen Sie im Schritt **Datenbankoption auswählen** die Option **Microsoft SQL Server Express** aus, und klicken Sie dann auf **Weiter**.



Bei Verwendung der Microsoft SQL Server Express-Datenbank mit ePolicy Orchestrator wird die Option zur Wiederherstellung nach einem Systemausfall automatisch deaktiviert. Aufgrund der Größenbeschränkungen für den Datenbankspeicher sollten Sie bei Verwendung dieser Datenbank die Option zur Wiederherstellung nach einem Systemausfall nicht aktivieren.

6 Im Schritt **Zusätzliche Software installieren** sind alle noch erforderlichen Komponenten aufgelistet. Klicken Sie für deren Installation auf **Weiter**.



Wenn SQL Express installiert wird, ist Microsoft .NET Framework 2.0 (oder höher) erforderlich. Diese Software wird nicht automatisch installiert. Wenn diese Software fehlt, müssen Sie das Setup beenden und die Software manuell installieren, bevor Sie fortfahren können.

7 Geben Sie im Schritt **Datenbankinformationen** Ihre Anmeldeinformationen für die Windows-Authentifizierung an, und klicken Sie dann auf **Weiter**.

8 Wenn es bei standardmäßig zugewiesenen Ports zu Konflikten kommt, müssen Sie diese beheben, indem Sie im Schritt **HTTP-Portinformationen** alternative Ports angeben.



Wenn keine Konflikte vorliegen, können Sie die Standardportzuweisungen nicht ändern. Wenn Sie Portzuweisungen ändern möchten, müssen Sie die Installationsoption **Benutzerdefiniert** auswählen.

9 Geben Sie diese Informationen im Schritt **Administratorinformationen** ein, und klicken Sie dann auf **Weiter**.

   a Geben Sie die Anmeldeinformationen (**Benutzername** und **Kennwort**) ein, die Sie für Ihr primäres Administratorkonto verwenden möchten.

   b Geben Sie je nach dem Typ der Installation das **Kennwort für die Schlüsselspeicherverschlüsselung** ein. Das heißt:
      - **Normale** oder **Erstinstallation** – Geben Sie ein Kennwort ein, mit dem Snapshot-Datensätze für die Wiederherstellung nach einem Systemausfall verschlüsselt werden.



Bewahren Sie dieses Kennwort gut auf. Falls Sie Ihre ePolicy Orchestrator-Datenbank wiederherstellen müssen, können Sie mit diesem Kennwort die Datensätze aus dem Snapshot für die Wiederherstellung nach einem Systemausfall entschlüsseln.

      - **Wiederherstellungsinstallation** – Geben Sie das Kennwort zum Entschlüsseln der Datensätze aus dem Snapshot für die Wiederherstellung nach einem Systemausfall ein. Ausführliche Informationen dazu finden Sie im *Produkthandbuch*.

10. Geben Sie im Schritt **Lizenzschlüssel eingeben** Ihren Lizenzschlüssel ein, und klicken Sie dann auf **Weiter**.

    Wenn Sie keinen Lizenzschlüssel besitzen, können Sie die Option **Test** auswählen, um mit der Installation der Software fortzufahren. Die Testphase ist auf 90 Tage begrenzt. Nach Abschluss der Installation können Sie einen Lizenzschlüssel innerhalb der Anwendung eingeben. Weitere Informationen hierzu finden Sie im Produkthandbuch oder in der Hilfe.

11. Erklären Sie sich mit dem **McAfee Endbenutzer-Lizenzvertrag** einverstanden, und klicken Sie auf **OK**.

12. Legen Sie im Dialogfeld **Bereit zum Installieren des Programms** fest, ob Sie **Anonyme Nutzungsinformationen an McAfee senden** möchten, und klicken Sie dann auf **Installieren**, um mit der Installation der Software zu beginnen.

    Wenn McAfee keine anonymen Diagnose- und Nutzungsdaten erfassen soll, deaktivieren Sie das Kontrollkästchen.

13. Klicken Sie nach Abschluss der Installation auf **Fertig stellen**, um den InstallShield-Assistenten zu beenden.

ePolicy Orchestrator ist nun installiert. Doppelklicken Sie auf Ihrem Desktop auf das Schildsymbol , um mit Ihrem McAfee ePO-Server zu arbeiten, oder wechseln Sie auf einer remoten Web-Konsole zu dem Server (https://<Server-Name>:<Port>).

Durchführen einer benutzerdefinierten Installation

Bei einer Installation vom Typ **Benutzerdefiniert** können Sie während der einzelnen Installationsschritte Änderungen vornehmen. So können Sie bei dieser Option zum Beispiel Zielordner oder Ports angeben.

Bevor Sie beginnen

Lesen, verstehen und befolgen Sie unbedingt die im Kapitel *Anforderungen und Empfehlungen für die Installation* aufgeführten Punkte.

Wenn Sie eine vorhandene SQL Server-Installation verwenden oder einen neuen SQL Server manuell installieren möchten, müssen Sie vor Beginn der Installation die folgenden Informationen ermitteln und die folgenden Schritte durchführen, um sicherzustellen, dass ePolicy Orchestrator mit dem Datenbank-Server kommunizieren kann:

1. Stellen Sie sicher, dass der **SQL Browser-Dienst** ausgeführt wird.
2. Stellen Sie sicher, dass im SQL Server-Konfigurations-Manager das TCP/IP-Protokoll aktiviert ist.
3. Aktualisieren Sie das System, das als Host für den McAfee ePO-Server dienen soll, und den SQL-Server mit den aktuellen Microsoft-Sicherheits-Updates, und deaktivieren Sie dann Windows-Updates für die Dauer der Installation.



Bei einer Installation vom Typ **Benutzerdefiniert** müssen Sie den gesamten Installationsvorgang überwachen. Möglicherweise müssen Sie das System neu starten.

Vorgehensweise

1. Melden Sie sich mit einem Konto, das über lokale Administratorrechte verfügt, bei dem Windows-Computer an, der als McAfee ePO-Server verwendet werden soll.
2. Bei Software, die Sie von der McAfee-Website heruntergeladen haben: Extrahieren Sie die Dateien in einen temporären Speicherort, und doppelklicken Sie auf `SETUP.EXE`. Die ausführbare Datei befindet sich in der heruntergeladenen ePolicy Orchestrator-Installationsdatei.

   Versuchen Sie nicht, die Datei `SETUP.EXE` auszuführen, bevor Sie den Inhalt der ZIP-Datei extrahiert haben.

   Der **McAfee ePolicy Orchestrator – InstallShield-Assistent** wird gestartet.
3. Klicken Sie auf eine der folgenden Optionen:
   - **Weiter**, wenn Sie eine normale ePolicy Orchestrator-Installation durchführen möchten.
   - **ePO aus einem vorhandenen Datenbank-Snapshot wiederherstellen** und **Weiter**, wenn Sie eine ePolicy Orchestrator-Wiederherstellungsinstallation durchführen möchten. Die ePolicy Orchestrator-Funktion "Snapshot für Wiederherstellung nach Systemausfall" ermöglicht nach einem Ausfall der Hardware, auf der sich der McAfee ePO-Server befindet, eine schnelle Wiederherstellung. Diese Funktion speichert die ePolicy Orchestrator-Konfiguration sowie Erweiterungen, Schlüssel und andere Informationen in Snapshot-Datensätzen in der ePolicy Orchestrator-Datenbank.

     Bei einer Wiederherstellungsinstallation werden einige Erstinstallations-Dialogfelder zur Datenbankauswahl nicht angezeigt.
4. Wählen Sie im Schritt **Setup-Typ** die Option **Benutzerdefiniert** aus, und klicken Sie dann auf **Weiter**.
5. Wählen Sie im Schritt **Datenbankoption auswählen** eine der folgenden Optionen aus, und klicken Sie dann auf **Weiter**:
   - **Microsoft SQL Server Express** – Installiert SQL Server 2008 Express automatisch in dem von Microsoft festgelegten Standardspeicherort (`C:\Programme\Microsoft SQL Server`).

     Bei Verwendung der Microsoft SQL Server Express-Datenbank mit ePolicy Orchestrator wird die Option zur Wiederherstellung nach einem Systemausfall automatisch deaktiviert. Aufgrund der Größenbeschränkungen für den Datenbankspeicher sollten Sie bei Verwendung dieser Datenbank die Option zur Wiederherstellung nach einem Systemausfall nicht aktivieren.
   - **Microsoft SQL Server** – Wählen Sie diese Option, um einen bereits installierten SQL-Datenbank-Server anzugeben.

     Bei Angabe eines bereits installierten Microsoft SQL-Datenbank-Servers wird die ePolicy Orchestrator-Funktion zur Wiederherstellung nach einem Systemausfall automatisch aktiviert. Weitere Informationen dazu finden Sie im *Produkthandbuch von ePolicy Orchestrator*.

     Wenn auf das Server-System, auf dem die Installation erfolgen soll, eine der folgenden Bedingungen zutrifft, kann SQL Server 2008 Express nicht lokal installiert werden:
     - Auf dem lokal installierten SQL-Server sind bereits 16 (oder mehr) benannte Instanzen vorhanden.
     - Es ist eine lokal installierte Version von SQL Server vorhanden, die eine Instanz mit dem Namen EPOSERVER enthält.
     - SQL Server 2008 Express ist bereits lokal installiert.

6 Im Schritt **Zusätzliche Software installieren** sind alle noch erforderlichen Komponenten aufgelistet. Klicken Sie für deren Installation auf **Weiter**.



Wenn SQL Express installiert wird, ist Microsoft .NET Framework 2.0 (oder höher) erforderlich. Diese Software wird nicht automatisch installiert. Wenn diese Software fehlt, müssen Sie das Setup beenden und die Software manuell installieren, bevor Sie fortfahren können.

7 Klicken Sie im Schritt **Zielordner** auf Folgendes:

- **Weiter** – Installieren Sie die McAfee ePO-Software im Standardspeicherort (`C:\Programme\McAfee\ePolicy Orchestrator\`).
- **Ändern** – Geben Sie einen benutzerdefinierten Zielspeicherort für McAfee ePO an. Wenn das Fenster **Aktuellen Zielordner ändern** geöffnet wird, wechseln Sie zum Zielordner, und erstellen Sie gegebenenfalls neue Ordner. Klicken Sie abschließend auf **OK**.

8 Führen Sie im Schritt **Datenbankinformationen** Folgendes durch:

- Wenn Sie **Microsoft SQL Server Express** ausgewählt haben, geben Sie Ihre Anmeldeinformationen für die Windows-Authentifizierung an, und klicken Sie dann auf **Weiter**.
- Wenn Sie **Microsoft SQL Server** ausgewählt haben:
  1 Wählen Sie den Server im Menü **Datenbank-Server** aus.
  2 Geben Sie an, welcher Typ von **Anmeldeinformationen für Datenbank-Server** verwendet werden soll, und klicken Sie dann auf **Weiter**:
    a Wählen Sie den Server im Menü **Datenbank-Server** aus.
    b Geben Sie an, welcher Typ von **Anmeldeinformationen für Datenbank-Server** verwendet werden soll, und klicken Sie dann auf **Weiter**:

Windows-Authentifizierung	1 Wählen Sie im Menü **Domäne** die Domäne des Benutzerkontos aus, das Sie zum Zugreifen auf den SQL-Server verwenden möchten. 2 Geben Sie **Benutzername** und **Kennwort** ein. Wenn Sie einen bereits installierten SQL-Server verwenden, müssen Sie sicherstellen, dass Ihr Benutzerkonto über Zugriffsberechtigungen verfügt.
SQL-Authentifizierung	• Geben Sie **Benutzername** und **Kennwort** für Ihren SQL-Server ein. Vergewissern Sie sich, dass die von Ihnen angegebenen Anmeldeinformationen einem im SQL-Server vorhandenen Benutzer mit entsprechenden Berechtigungen gehören. Bei Verwendung von SQL-Authentifizierung ist das Menü **Domäne** ausgegraut.



Möglicherweise müssen Sie den **TCP-Port für SQL-Server** eingeben, über den die Kommunikation zwischen dem McAfee ePO-Server und dem Datenbank-Server erfolgen soll (die Standardports für diese Kommunikation sind 1433 oder 1434).

9 Überprüfen Sie im Schritt **HTTP-Portinformationen** die standardmäßig zugewiesenen Ports. Klicken Sie auf **Weiter**, um zu überprüfen, dass diese Ports auf dem System nicht bereits belegt sind.



Einige dieser Ports können Sie jetzt ändern. Nach Abschluss der Installation können Sie nur den **Kommunikationsport für Agenten-Reaktivierung** und den **Kommunikationsport für Agenten-Übertragung** ändern. Wenn Sie die anderen Porteinstellungen zu einem späteren Zeitpunkt ändern möchten, müssen Sie McAfee ePO neu installieren. Weitere Informationen zum Ändern von Portwerten finden Sie unter *Informationen zu HTTP-Port-Optionen*.

10 Geben Sie diese Informationen im Schritt **Informationen zum globalen Administrator** ein, und klicken Sie dann auf **Weiter**.

   a Geben Sie die Anmeldeinformationen (**Benutzername** und **Kennwort**) ein, die Sie für Ihr primäres Konto des globalen Administrators verwenden möchten.

   b Geben Sie je nach dem Typ der Installation das **Kennwort für die Schlüsselspeicherverschlüsselung** ein. Das heißt:

   - **Normale** oder **Erstinstallation** – Geben Sie ein Kennwort ein, mit dem Snapshot-Datensätze für die Wiederherstellung nach einem Systemausfall verschlüsselt werden.

     Bewahren Sie dieses Kennwort gut auf. Falls Sie Ihre ePolicy Orchestrator-Datenbank wiederherstellen müssen, können Sie mit diesem Kennwort die Datensätze aus dem Snapshot für die Wiederherstellung nach einem Systemausfall entschlüsseln.

   - **Wiederherstellungsinstallation** – Geben Sie das Kennwort zum Entschlüsseln der Datensätze aus dem Snapshot für die Wiederherstellung nach einem Systemausfall ein. Ausführliche Informationen dazu finden Sie im *Produkthandbuch*.

11 Geben Sie im Schritt **Lizenzschlüssel eingeben** Ihren Lizenzschlüssel ein, und klicken Sie dann auf **Weiter**.

   Wenn Sie keinen Lizenzschlüssel besitzen, können Sie die Option **Test** auswählen, um mit der Installation der Software fortzufahren. Die Testphase ist auf 90 Tage begrenzt. Nach Abschluss der Installation können Sie einen Lizenzschlüssel innerhalb der Anwendung eingeben. Weitere Informationen hierzu finden Sie im *Produkthandbuch* oder in der Hilfe.

12 Erklären Sie sich mit dem **McAfee Endbenutzer-Lizenzvertrag** einverstanden, und klicken Sie auf **OK**.

13 Legen Sie im Dialogfeld **Bereit zum Installieren des Programms** fest, ob Sie **Anonyme Nutzungsinformationen an McAfee senden** möchten, und klicken Sie dann auf **Installieren**, um mit der Installation der Software zu beginnen.

   Wenn McAfee keine anonymen Diagnose- und Nutzungsdaten erfassen soll, deaktivieren Sie das Kontrollkästchen.

14 Nach Abschluss der Installation klicken Sie auf **Fertig stellen**, um den InstallShield-Assistenten zu beenden.

ePolicy Orchestrator ist nun installiert. Doppelklicken Sie auf Ihrem Desktop auf das Schildsymbol , um mit Ihrem McAfee ePO-Server zu arbeiten, oder wechseln Sie auf einer remoten Web-Konsole zu dem Server (https://<Server-Name>:<Port>)

Durchführen einer Cluster-Installation

ePolicy Orchestrator bietet hohe Verfügbarkeit für Server-Cluster mit Microsoft Cluster Server (MSCS).

Beim Installieren der Software in einer MSCS-Umgebung müssen zusätzlich zu den bei Installationen vom Typ **Express** und **Benutzerdefiniert** erforderlichen Schritten noch weitere Schritte durchgeführt werden. Der Installationsvorgang richtet sich danach, auf welchem Betriebssystem die Software installiert wird. Cluster-Installationen werden unter Windows Server 2008 oder Windows Server 2012 unterstützt.

Eine erfolgreiche Installation hängt von der korrekten Einrichtung der MSCS-Software (Microsoft Cluster Server) ab. Weitere Informationen zur MSCS-Einrichtung finden Sie in der Microsoft-Dokumentation.



Cluster.exe ist ein veralteter Befehl in Windows Server 2012. Installieren Sie während der Cluster-Einrichtung in Windows Server 2012 die Failovercluster-Befehlsschnittstelle als zusätzliche Funktion.

Terminologie für Cluster-Installationen

In Anweisungen zur Installation auf einem Cluster werden die folgenden Begriffe verwendet.

Tabelle 2-1 Terminologie für Cluster-Installationen

Begriff	Definition
Datenlaufwerk	Eines der beiden von Microsoft Cluster Server und ePolicy Orchestrator benötigten Laufwerke. Das Datenlaufwerk ist ein Remote-Laufwerk, auf das alle Knoten im Cluster zugreifen können, und es ist der Speicherort, in dem die ePolicy Orchestrator-Dateien installiert werden.
Virtuelle IP-Adresse für ePO (Ressource)	Das ist die IP-Adressressource, die Sie im Rahmen der Cluster-Installation von ePolicy Orchestrator erstellen. Diese virtuelle IP-Adresse steht für die McAfee ePO-Cluster-Installation als Ganzes. Verweise auf diese IP-Adresse zeigen auf den aktuell aktiven Knoten in Ihrem Cluster.
Virtueller Netzwerkname für ePO (Ressource)	Das ist die Netzwerknamenressource, die Sie im Rahmen der Cluster-Installation von ePolicy Orchestrator erstellen. Dieser virtuelle Netzwerkname steht für die McAfee ePO-Cluster-Installation als Ganzes. Verweise auf diesen Netzwerknamen zeigen auf den aktuell aktiven Knoten in Ihrem Cluster.
Quorum-Laufwerk	Eines der beiden von Microsoft Cluster Server benötigten Laufwerke. Auf dem Quorum-Laufwerk sind die MSCS-Dateien installiert. Installieren Sie auf diesem Laufwerk keine Dateien von ePolicy Orchestrator.

Erforderliche Komponenten für die Cluster-Installation

Vor Beginn einer Cluster-Installation sollten Sie diese Liste von Anforderungen und erforderlichen Komponenten lesen und sich vergewissern, dass alle aufgeführten Punkte vorhanden oder die Informationen verfügbar sind. Diese Anforderungen gelten sowohl für Installationen auf Windows Server 2008 als auch auf Windows Server 2012.

- Microsoft Cluster Server ist eingerichtet und wird in einem Cluster aus mindestens zwei Servern ausgeführt.
- Ein Quorum-Laufwerk ist vorhanden und gemäß Microsoft-Richtlinien konfiguriert.
- Ein Datenlaufwerk ist vorhanden und für alle im Cluster befindlichen Knoten verfügbar.
- Ein unterstützter remoter SQL-Server ist konfiguriert.

  So überprüfen Sie, dass ePolicy Orchestrator während der Installation mit diesem Server kommunizieren kann:

  - Stellen Sie sicher, dass der **SQL Browser-Dienst** ausgeführt wird.
  - Stellen Sie sicher, dass im SQL Server-Konfigurations-Manager das TCP/IP-Protokoll aktiviert ist.

- Während des Installationsvorgangs müssen Sie (je nach Ihrer Konfiguration) möglicherweise die folgenden Informationen auf der Seite **Datenbankinformationen** angeben:
  - Den Namen des SQL-Servers. Je nach Konfiguration sollte dieser Name unter Verwendung des SQL-Server-Namens oder des SQL-Server-Namens *und* des Instanznamens angegeben werden.
  - Die vom SQL-Server verwendete dynamische Portnummer (sofern vorhanden). Die dynamische Portnummer geben Sie während des Installationsvorgangs auf der Seite **Datenbankinformationen** an.

Installieren auf einem System mit Windows Server 2008

Wenn Sie ePolicy Orchestrator in einer Cluster-Umgebung mit Windows Server 2008-Systemen installieren, müssen Sie alle folgenden Schritte in der aufgeführten Reihenfolge ausführen.

Bevor Sie beginnen

Aktualisieren Sie die Systeme, die als Host für den ePolicy Orchestrator-Server dienen sollen, und den SQL-Server mit den aktuellen Microsoft-Sicherheits-Updates, und deaktivieren Sie dann Windows-Updates für die Dauer der Installation.

Aufgaben

- *Erstellen der ePolicy Orchestrator-Anwendungsgruppe* auf Seite 25

  Die Anwendungsgruppe "ePolicy Orchestrator" ist erforderlich, um die Anwendung ePolicy Orchestrator in einer Cluster-Umgebung von den Microsoft Cluster-Diensten (Microsoft Cluster Services, MSCS) zu trennen.
- *Erstellen des Client-Zugriffspunkts* auf Seite 26

  Der Client-Zugriffspunkt definiert die virtuelle IP-Adresse und die virtuellen Netzwerknamen von ePolicy Orchestrator, damit die Cluster-Knoten mit dem McAfee ePO-Server kommunizieren können.
- *Hinzufügen des Datenlaufwerks* auf Seite 26

  Das Datenlaufwerk ist der Speicherort, in dem ePolicy Orchestrator installiert wird. Verwenden Sie ein Remote-Laufwerk, auf das von allen Knoten im Cluster zugegriffen werden kann.
- *Installieren von ePolicy Orchestrator auf jedem Knoten* auf Seite 26

  Führen Sie die **Cluster**-Installation auf jedem Knoten des Clusters aus. Damit sichergestellt ist, dass jeder Knoten während der Installation über exklusiven Zugriff auf die Quorum- und Datenlaufwerke verfügt, müssen Sie alle anderen Knoten im Cluster herunterfahren.
- *Erstellen der Ressourcen "Allgemeiner Dienst"* auf Seite 27

  Mithilfe der Ressourcen "Allgemeiner Dienst" kann der Cluster-Server den ePolicy Orchestrator-Server durch Starten und Anhalten der ePolicy Orchestrator-Dienste steuern.

Erstellen der ePolicy Orchestrator-Anwendungsgruppe

Die Anwendungsgruppe "ePolicy Orchestrator" ist erforderlich, um die Anwendung ePolicy Orchestrator in einer Cluster-Umgebung von den Microsoft Cluster-Diensten (Microsoft Cluster Services, MSCS) zu trennen.

Vorgehensweise

1. Öffnen Sie das Tool zur Failover-Clusterverwaltung auf dem aktiven Knoten, indem Sie auf **Start** | **Programme** | **Verwaltung** | **Failover-Clusterverwaltung** klicken.
2. Klicken Sie in der Cluster-Verwaltungsstruktur mit der rechten Maustaste auf **Dienste und Anwendungen**, und wählen Sie dann **Weitere Aktionen** | **Leeren Dienst oder leere Anwendung erstellen** aus.
3. Klicken Sie mit der rechten Maustaste auf **Neuer Dienst oder neue Anwendung**, und wählen Sie **Umbenennen** aus, um die Anwendungsgruppe in `ePO` umzubenennen.

Erstellen des Client-Zugriffspunkts

Der Client-Zugriffspunkt definiert die virtuelle IP-Adresse und die virtuellen Netzwerknamen von ePolicy Orchestrator, damit die Cluster-Knoten mit dem McAfee ePO-Server kommunizieren können.

Vorgehensweise

1. Klicken Sie mit der rechten Maustaste auf die Gruppe **ePO**, und wählen Sie **Ressource hinzufügen** | **Client-Zugriffspunkt** aus. Der Assistent für Client-Zugriffspunkte wird angezeigt.
2. Geben Sie den **Virtuellen Namen für ePolicy Orchestrator** in das Feld **Name** und die **Virtuelle IP-Adresse für ePolicy Orchestrator** in das Feld **Adresse** ein, und klicken Sie anschließend auf **Weiter**. Die Seite **Bestätigung** wird angezeigt.
3. Klicken Sie auf **Weiter**, damit der **Client-Zugriffspunkt** konfiguriert werden kann, und klicken Sie nach Abschluss des Assistenten auf **Fertig stellen**.
4. Wenn der **Client-Zugriffspunkt** offline ist, klicken Sie mit der rechten Maustaste auf den Namen, und wählen Sie **Diese Ressource online schalten** aus.

Hinzufügen des Datenlaufwerks

Das Datenlaufwerk ist der Speicherort, in dem ePolicy Orchestrator installiert wird. Verwenden Sie ein Remote-Laufwerk, auf das von allen Knoten im Cluster zugegriffen werden kann.

Vorgehensweise

1. Klicken Sie mit der rechten Maustaste auf die Anwendungsgruppe **ePO**, und wählen Sie **Speicher hinzufügen** aus.
2. Wählen Sie im Dialogfeld **Speicher hinzufügen** das Datenlaufwerk aus, das für Ihre ePolicy Orchestrator-Installation verwendet werden soll, und klicken Sie dann auf **OK**.

Installieren von ePolicy Orchestrator auf jedem Knoten

Führen Sie die **Cluster**-Installation auf jedem Knoten des Clusters aus. Damit sichergestellt ist, dass jeder Knoten während der Installation über exklusiven Zugriff auf die Quorum- und Datenlaufwerke verfügt, müssen Sie alle anderen Knoten im Cluster herunterfahren.

Vorgehensweise

1. Doppelklicken Sie im Installationsordner auf `SETUP.EXE`.
2. Folgen Sie den Anweisungen des Assistenten, bis Sie zur Seite **Setup-Typ** gelangen. Wählen Sie dort die Option **Cluster** aus, und klicken Sie dann auf **Weiter**.
3. Geben Sie auf der Seite **Zielverzeichnis auswählen** den Pfad für das freigegebene Datenlaufwerk ein, und klicken Sie dann auf **Weiter**.

   
   Verwenden Sie für jeden Knoten denselben Pfad.

4. Geben Sie auf der Seite **Einstellungen für virtuellen Server festlegen** (nur auf dem ersten Knoten) die folgenden Identifizierungsinformationen für den McAfee ePO-Cluster an:
   - Die IP-Adresse des virtuellen ePolicy Orchestrator-Servers
   - Den Namen des virtuellen ePolicy Orchestrator-Clusters
   - Den vollqualifizierten Domänennamen (FQDN) des virtuellen ePolicy Orchestrator-Clusters

   
   Diese Informationen werden automatisch auf nachfolgenden Knoten bereitgestellt.

5 Führen Sie die Installation auf dem ersten Knoten wie unter *Durchführen einer benutzerdefinierten Installation* beschrieben durch.

6 Wiederholen Sie diese Schritte für jeden Knoten im Cluster.

Erstellen der Ressourcen "Allgemeiner Dienst"

Mithilfe der Ressourcen "Allgemeiner Dienst" kann der Cluster-Server den ePolicy Orchestrator-Server durch Starten und Anhalten der ePolicy Orchestrator-Dienste steuern.

Fügen Sie drei Ressourcen "Allgemeiner Dienst" hinzu, die mit Ihrem geclusterten ePolicy Orchestrator-Server verwendet werden sollen. Gehen Sie zum Konfigurieren der einzelnen Ressourcen anhand der folgenden Tabelle und Vorgehensweisen vor. Erstellen Sie dabei die Ressourcen in der Reihenfolge, in der sie in der Tabelle aufgeführt sind.

Ressource	Eigenschaften: Registerkarte "Allgemein"	Eigenschaften: Registerkarte "Abhängigkeiten"
ePolicy Orchestrator 5.0.0-Anwendungs-Server	Keine Änderungen erforderlich	Datenlaufwerk
ePolicy Orchestrator 5.0.0-Server	Entfernen Sie die **Startparameter**, und fügen Sie ein Leerzeichen hinzu. Wenn Startparameter angegeben sind, startet Apache nicht, und ein leerer Eintrag ist nicht zulässig. Deshalb ist ein Leerzeichen erforderlich.	ePolicy Orchestrator 5.0.0-Anwendungs-Server
ePolicy Orchestrator 5.0.0-Ereignisanalyse	Keine Änderungen erforderlich	ePolicy Orchestrator 5.0.0-Anwendungs-Server

Vorgehensweise

1 Klicken Sie in der Cluster-Verwaltung mit der rechten Maustaste auf die Anwendungsgruppe **ePO**, und wählen Sie **Ressource hinzufügen** | **Allgemeiner Dienst** aus.

2 Wählen Sie im Assistenten zum Auswählen von Diensten eine Ressource aus, und klicken Sie auf **Weiter**.

3 Klicken Sie auf der Seite **Bestätigung** auf **Weiter**, damit der Dienst erstellt werden kann. Klicken Sie nach Abschluss des Assistenten auf **Fertig stellen**.

4 Klicken Sie mit der rechten Maustaste auf die von Ihnen erstellte Ressource, und wählen Sie **Eigenschaften** aus. Legen Sie im Dialogfeld **Eigenschaften** die Eigenschaften fest, die in der Konfigurationstabelle für die Ressource "Allgemeiner Dienst" angegeben sind.

5 Wiederholen Sie diese Schritte für jede einzelne Ressource "Allgemeiner Dienst".

Installieren auf einem System mit Windows Server 2012

Wenn Sie ePolicy Orchestrator in einer Cluster-Umgebung mit Windows Server 2012-Systemen installieren, müssen Sie alle folgenden Schritte in der aufgeführten Reihenfolge ausführen.

> **Bevor Sie beginnen**
>
> Aktualisieren Sie die Systeme, die als Host für den ePolicy Orchestrator-Server dienen sollen, und den SQL-Server mit den aktuellen Microsoft-Sicherheits-Updates, und deaktivieren Sie dann Windows-Updates für die Dauer der Installation.

Aufgaben

- *Erstellen der ePolicy Orchestrator-Anwendungsrolle* auf Seite 28
  Die Anwendungsrolle "ePolicy Orchestrator" ist erforderlich, um die Anwendung ePolicy Orchestrator in einer Cluster-Umgebung von den Microsoft Cluster-Diensten (Microsoft Cluster Services, MSCS) zu trennen.
- *Erstellen des Client-Zugriffspunkts* auf Seite 29
  Der Client-Zugriffspunkt definiert die virtuelle IP-Adresse und die virtuellen Netzwerknamen von ePolicy Orchestrator, damit die Cluster-Knoten mit dem McAfee ePO-Server kommunizieren können.
- *Hinzufügen des Datenlaufwerks* auf Seite 29
  Das Datenlaufwerk ist der Speicherort, an dem ePolicy Orchestrator installiert wird. Verwenden Sie ein Remote-Laufwerk, auf das von allen Knoten im Cluster zugegriffen werden kann.
- *Installieren von ePolicy Orchestrator auf jedem Knoten* auf Seite 29
  Führen Sie die **Cluster**-Installation auf jedem Knoten des Clusters aus. Damit sichergestellt ist, dass jeder Knoten während der Installation über exklusiven Zugriff auf die Quorum- und Datenlaufwerke verfügt, müssen Sie alle anderen Knoten im Cluster herunterfahren.
- *Erstellen der Ressourcen "Allgemeiner Dienst"* auf Seite 30
  Mithilfe der Ressourcen "Allgemeiner Dienst" kann der Cluster-Server den ePolicy Orchestrator-Server durch Starten und Anhalten der ePolicy Orchestrator-Dienste steuern.

Erstellen der ePolicy Orchestrator-Anwendungsrolle

Die Anwendungsrolle "ePolicy Orchestrator" ist erforderlich, um die Anwendung ePolicy Orchestrator in einer Cluster-Umgebung von den Microsoft Cluster-Diensten (Microsoft Cluster Services, MSCS) zu trennen.

Vorgehensweise

1. Öffnen Sie den Failovercluster-Manager. Klicken Sie dazu auf **Server-Manager** | **Extras** | **Failovercluster-Manager**.
2. Klicken Sie mit der rechten Maustaste in der Systemstruktur auf **Rollen**, und wählen Sie dann **Leere Rolle erstellen** aus.
3. Klicken Sie auf **OK**.
4. Klicken Sie mit der rechten Maustaste auf die leere Rolle, und wählen Sie dann **Eigenschaften** aus.
5. Geben Sie im Dialogfeld **Neue Rolle** den **Namen** für die Rolle ein. Zum Beispiel: `ePO`.
6. Klicken Sie auf **OK**.

Erstellen des Client-Zugriffspunkts

Der Client-Zugriffspunkt definiert die virtuelle IP-Adresse und die virtuellen Netzwerknamen von ePolicy Orchestrator, damit die Cluster-Knoten mit dem McAfee ePO-Server kommunizieren können.

Vorgehensweise

1. Klicken Sie mit der rechten Maustaste auf die Anwendungsrolle **ePO**, und wählen Sie dann **Ressource hinzufügen | Client-Zugriffspunkt** aus. Der Assistent für Client-Zugriffspunkte wird angezeigt.
2. Geben Sie den **Virtuellen Namen für ePolicy Orchestrator** in das Feld **Name** sowie die **Virtuelle IP-Adresse für ePolicy Orchestrator** in das Feld **Adresse** ein, und klicken Sie anschließend auf **Weiter**. Die Seite **Bestätigung** wird angezeigt.
3. Klicken Sie auf **Weiter**, um die Änderungen am **Client-Zugriffspunkt** zu übernehmen, und klicken Sie abschließend auf **Fertig stellen**.
4. Wenn der **Client-Zugriffspunkt** offline ist, klicken Sie mit der rechten Maustaste auf den Namen, und wählen Sie **Online schalten** aus.

Hinzufügen des Datenlaufwerks

Das Datenlaufwerk ist der Speicherort, an dem ePolicy Orchestrator installiert wird. Verwenden Sie ein Remote-Laufwerk, auf das von allen Knoten im Cluster zugegriffen werden kann.

Vorgehensweise

1. Klicken Sie mit der rechten Maustaste auf die Anwendungsrolle **ePO**, und wählen Sie **Speicher hinzufügen** aus.
2. Wählen Sie im Dialogfeld **Speicher hinzufügen** das Datenlaufwerk aus, das für Ihre ePolicy Orchestrator-Installation verwendet werden soll, und klicken Sie dann auf **OK**.

Installieren von ePolicy Orchestrator auf jedem Knoten

Führen Sie die **Cluster**-Installation auf jedem Knoten des Clusters aus. Damit sichergestellt ist, dass jeder Knoten während der Installation über exklusiven Zugriff auf die Quorum- und Datenlaufwerke verfügt, müssen Sie alle anderen Knoten im Cluster herunterfahren.

Vorgehensweise

1. Doppelklicken Sie im Installationsordner auf `SETUP.EXE`.
2. Folgen Sie den Anweisungen des Assistenten, bis Sie zur Seite **Setup-Typ** gelangen. Wählen Sie dort die Option **Cluster** aus, und klicken Sie dann auf **Weiter**.
3. Geben Sie auf der Seite **Zielverzeichnis auswählen** den Pfad für das freigegebene Datenlaufwerk ein, und klicken Sie dann auf **Weiter**. Wenn der von Ihnen angegebene Ordner nicht vorhanden ist, wird bei der Installation ein neuer Ordner mit diesem Namen im angegebenen Speicherort erstellt.

   
   Verwenden Sie für jeden Knoten denselben Pfad.

4. Geben Sie auf der Seite **Einstellungen für virtuellen Server festlegen** (nur auf dem ersten Knoten) die folgenden Identifizierungsinformationen für den McAfee ePO-Cluster an:
   - Die IP-Adresse des virtuellen ePolicy Orchestrator-Servers
   - Den Namen des virtuellen ePolicy Orchestrator-Clusters
   - Den vollqualifizierten Domänennamen (FQDN) des virtuellen ePolicy Orchestrator-Clusters

   
   Diese Informationen werden automatisch auf nachfolgenden Knoten bereitgestellt.

5. Führen Sie die Installation auf dem ersten Knoten wie unter *Durchführen einer benutzerdefinierten Installation* beschrieben durch.

6. Wiederholen Sie diese Schritte für jeden Knoten im Cluster.

Erstellen der Ressourcen "Allgemeiner Dienst"

Mithilfe der Ressourcen "Allgemeiner Dienst" kann der Cluster-Server den ePolicy Orchestrator-Server durch Starten und Anhalten der ePolicy Orchestrator-Dienste steuern.

Fügen Sie drei Ressourcen "Allgemeiner Dienst" hinzu, die mit Ihrem geclusterten ePolicy Orchestrator-Server verwendet werden sollen. Gehen Sie zum Konfigurieren der einzelnen Ressourcen anhand der folgenden Tabelle und Vorgehensweisen vor. Erstellen Sie dabei die Ressourcen in der Reihenfolge, in der sie in der Tabelle aufgeführt sind.

Ressource	Eigenschaften: Registerkarte "Allgemein"	Eigenschaften: Registerkarte "Abhängigkeiten"
ePolicy Orchestrator 5.0.0-Anwendungs-Server	Keine Änderungen erforderlich	ePolicy Orchestrator 5.0.0-Server
ePolicy Orchestrator 5.0.0-Server	Entfernen Sie die **Startparameter**, und fügen Sie ein Leerzeichen hinzu. Wenn Startparameter angegeben sind, startet Apache nicht, und ein leerer Eintrag ist nicht zulässig. Deshalb ist ein Leerzeichen erforderlich.	Keine Änderungen erforderlich
ePolicy Orchestrator 5.0.0-Ereignisanalyse	Keine Änderungen erforderlich	ePolicy Orchestrator 5.0.0-Anwendungs-Server

Vorgehensweise

1. Klicken Sie in der Cluster-Verwaltung mit der rechten Maustaste auf die Anwendungsrolle **ePO**, und wählen Sie dann **Ressource hinzufügen** | **Allgemeiner Dienst** aus.

   Der Assistent zum Erstellen neuer Ressourcen wird angezeigt.

2. Wählen Sie eine Ressource aus, und klicken Sie dann auf **Weiter**.

3. Klicken Sie auf der Seite **Bestätigung** auf **Weiter**, um den Dienst zu erstellen. Klicken Sie abschließend auf **Fertig stellen**.

4. Klicken Sie mit der rechten Maustaste auf die Ressource, und wählen Sie dann **Eigenschaften** aus. Legen Sie im Dialogfeld **Eigenschaften** die Eigenschaften fest, die in der Konfigurationstabelle für die Ressource "Allgemeiner Dienst" angegeben sind.

5. Wiederholen Sie diese Schritte für jede einzelne Ressource "Allgemeiner Dienst".

Testen der ePolicy Orchestrator-Cluster-Installation

Gehen Sie wie nachfolgend beschrieben vor, um nach dem Einrichten und Aktivieren des ePolicy Orchestrator-Clusters sicherzustellen, dass die Software bei einem Failover funktioniert.

Vorgehensweise

1. Starten Sie das System neu, das als aktiver Knoten dient. Der passive Knoten wird automatisch zum aktiven Knoten.

   Die Zeitspanne, bis der passive Knoten zum aktiven Knoten wird, hängt von der jeweiligen Umgebung ab.

2. Aktualisieren Sie Ihre Browser-Sitzung manuell. Wenn der Failover-Vorgang erfolgreich war, werden Sie auf die ePolicy Orchestrator-Anmeldeseite geleitet.

Installation remoter Agentensteuerungen

Auf jedem ePolicy Orchestrator-Server befindet sich eine Master-Agentensteuerung. Durch Installation zusätzlicher remoter Agentensteuerungen kann eine größere Anzahl von Produkten und Systemen von einem einzigen logischen ePolicy Orchestrator-Server verwaltet werden, vorausgesetzt, die CPU auf dem Datenbank-Server wird nicht überlastet.

Remote Agentensteuerungen benötigen denselben Hochgeschwindigkeits-Netzwerkzugriff auf die Datenbank wie der primäre ePolicy Orchestrator-Server.



Sie können für die Agent-zu-Server-Kommunikation zusätzliche IP-Adressen verwenden, indem Sie eine Agentensteuerungsgruppe erstellen und die zusätzliche IP-Adresse zum Eingabefeld für virtuelle IP-Adressen hinzufügen. Weitere Informationen dazu finden Sie unter *Arbeiten mit Agentensteuerungen* im Produkthandbuch oder in der Hilfe.

Installieren remoter Agentensteuerungen

Sie können in Ihrer Umgebung Agentensteuerungen installieren, um die Agent-zu-Server-Kommunikation und den Lastausgleich besser verwalten zu können. Remote Agentensteuerungen können Sie zu jedem beliebigen Zeitpunkt installieren.

Bevor Sie beginnen

Aktualisieren Sie das System mit den aktuellen Microsoft-Sicherheits-Updates, und deaktivieren Sie dann Windows-Updates für die Dauer der Installation.

Vorgehensweise

1. Öffnen Sie den Ordner, in den Sie den Inhalt des ePolicy Orchestrator-Installationspakets extrahiert haben.
2. Kopieren Sie den Ordner `Agent Handler` auf das gewünschte Server-System für die Agentensteuerung.
3. Doppelklicken Sie auf **SETUP.EXE**, um den McAfee-InstallShield-Assistenten für Agentensteuerungen zu starten. Nach einigen Installationsaktivitäten im Hintergrund wird der InstallShield-Assistent gestartet. Klicken Sie auf **Weiter**, um mit der Installation zu beginnen.
4. Nachdem Sie die Bedingungen des Lizenzvertrags akzeptiert haben, wird der Schritt **Zielordner** geöffnet.

5 Akzeptieren Sie das Standardziel, oder klicken Sie auf **Ändern**, um das Ziel zu ändern, und klicken Sie dann auf **Weiter**.



Der Zielpfad darf keine Doppelbytezeichen enthalten. Dies ist eine Einschränkung des Apache-Web-Servers. Die Verwendung von Doppelbytezeichen würde dazu führen, dass die Installation fehlschlägt und der Apache-Web-Server nicht startet.

6 Die Seite mit den Server-Informationen wird geöffnet.

a Geben Sie den Computernamen des McAfee ePO-Servers ein, mit dem die Agentensteuerung kommunizieren soll.

b Geben Sie den Port an, über den die Kommunikation von der Agentensteuerung zum Server erfolgen soll. Der Standardport ist 8444 – der gleiche wie der **Port für authentifizierte Client-zu-Server-Kommunikation**.



Bei Verwendung des Standardports kann die Kommunikation von der Agentensteuerung zum Server über einen einzigen Port (8444) erfolgen. Optional können Sie auch den Port 8443 (**Konsolen-Port zur Anwendungs-Server-Kommunikation**) angeben. In diesem Fall muss aber der Port 8444 weiterhin für die Agentensteuerungs-Kommunikation verfügbar sein.

c Geben Sie als ePO-Administratorinformationen den **Benutzernamen** und das **Kennwort** eines Benutzers mit globalen Administratorrechten für ePolicy Orchestrator ein.

d Klicken Sie auf **Weiter**, damit die **ePO-Administrator**-Anmeldeinformationen auch für den Zugriff auf die Datenbank verwendet werden. Stellen Sie dabei sicher, dass diesen die entsprechende SQL Server-Rolle und die entsprechenden SQL Server-Berechtigungen zugewiesen sind.

e Deaktivieren Sie **Anmeldeinformationen für ePO-Server-Datenbank verwenden**, und klicken Sie auf **Weiter**, wenn für den Zugriff auf die Datenbank andere Anmeldeinformationen verwendet werden sollen. Geben Sie auf der Seite **Datenbankinformationen** die folgenden Informationen an, und klicken Sie auf **Weiter**:

- **Datenbank-Server** mit Instanzname. Zum Beispiel: `DB-SERVER\SERVER-NAME`.
- Authentifizierungstyp.
- Name der **Domäne**, in der sich der Datenbank-Server befindet.
- **Benutzername** und **Kennwort**.
- **Datenbankname** (sofern nicht automatisch angegeben).

7 Klicken Sie auf **Installieren**, um mit der Installation zu beginnen. Nach Abschluss der Installation müssen Sie die remote Agentensteuerung auf der Benutzeroberfläche von ePolicy Orchestrator aktivieren. Weitere Informationen zum Aktivieren einer remoten Agentensteuerung finden Sie unter *Arbeiten mit Agentensteuerungen* im Produkthandbuch oder in der Hilfe.

Abschließen einer Erstinstallation

Nach Abschluss des Installationsvorgangs müssen Sie den ePolicy Orchestrator-Server konfigurieren.

Das Einrichten des Servers und der verwalteten Umgebung können Sie mithilfe der geführten Konfiguration von ePolicy Orchestrator vornehmen. Dieses Konfigurations-Tool umfasst vorhandene Features und Funktionen und soll Ihnen helfen, Ihren Server schnell und einfach zum Laufen zu bringen. Weitere Informationen dazu finden Sie unter *Verwenden des Tools zur geführten Konfiguration* im *Produkthandbuch von McAfee ePolicy Orchestrator* oder in der Hilfe.

3 Wiederherstellen von McAfee ePolicy Orchestrator

Sie können ePolicy Orchestrator in Form einer Wiederherstellungsinstallation wiederherstellen, bei der Ihr Microsoft SQL Server bereits über eine ePolicy Orchestrator-Konfiguration aus einer vorherigen Installation verfügt.

Falls Sie stattdessen eine Erstinstallation durchführen möchten, finden Sie weitere Informationen unter *Installieren von McAfee ePolicy Orchestrator*.

Inhalt

Optionen für eine Wiederherstellungsinstallation

Es gibt drei Optionen für eine Wiederherstellungsinstallation von ePolicy Orchestrator. Bei jeder dieser Optionen werden Sie vom InstallShield-Assistenten von ePolicy Orchestrator durch den Vorgang zur Wiederherstellungsinstallation geführt.



Vor einer Wiederherstellung von ePolicy Orchestrator müssen Sie die Sicherungsdatei für die SQL-Datenbank, in der sich die Datensätze aus dem Snapshot für die Wiederherstellung nach einem Systemausfall befinden, auf dem SQL-Wiederherstellungs-Server wiederherstellen. Ausführliche Informationen dazu finden Sie in der Dokumentation zu Microsoft SQL Server.

Welche Wiederherstellungsoption für Ihre Umgebung geeignet ist, können Sie mithilfe der folgenden Tabelle bestimmen.

Installationsoption	Details
Express	Die direkteste Installationsweise. Wählen Sie diese Option, wenn Sie für Ihre Installation die Standardeinstellungen von McAfee übernehmen möchten.
Benutzerdefiniert	Hierbei können Sie die Installation nach Ihren Wünschen anpassen. Wählen Sie diese Option aus, wenn Sie die Details der Installation beeinflussen möchten, wie zum Beispiel: • Den Zielordner, in dem die Software installiert werden soll (standardmäßig: `C:\Programme\McAfee\ePolicy Orchestrator\`). • Die zu verwendenden Ports. Die Installation von SQL Server 2008 Express ist optional. Sie können auch eine andere unterstützte SQL Server-Version angeben, sofern diese bereits vor Beginn der Installation von McAfee ePO installiert wurde.
Cluster	Führt eine Cluster-Installation durch. Wählen Sie diese Option aus, wenn Sie die Software in einer Cluster-Umgebung installieren möchten. Vor Beginn der Installation der Software müssen Sie Folgendes sicherstellen: • Ihre MSCS-Umgebung (Microsoft Cluster Server) muss eingerichtet sein. • Eine unterstützte SQL Server-Version muss in einem Speicherort installiert sein, auf den der Cluster zugreifen kann.



Wenn Sie eine frühere Version von McAfee ePolicy Orchestrator aktualisieren oder von einer Testversion migrieren, lesen Sie das Kapitel *Aktualisieren von McAfee ePolicy Orchestrator*.

Installieren von ePolicy Orchestrator auf dem Wiederherstellungs-Server

Für eine erneute Erstellung des McAfee ePO-Servers installieren Sie ePolicy Orchestrator auf einem Server neu und erstellen dann eine Verknüpfung zur wiederhergestellten SQL-Datenbank.

Bevor Sie beginnen

Lesen, verstehen und befolgen Sie unbedingt die im Kapitel *Anforderungen und Empfehlungen für die Installation* aufgeführten Punkte.

Wenn Sie den vorhandenen SQL-Server auswählen, müssen Sie vor Beginn der Installation die folgenden Informationen sammeln und die folgenden Schritte durchführen, um sicherzustellen, dass McAfee ePO mit dem Datenbank-Server kommunizieren kann:

1. Stellen Sie sicher, dass der **SQL Browser-Dienst** ausgeführt wird.
2. Stellen Sie sicher, dass im SQL Server-Konfigurations-Manager das TCP/IP-Protokoll aktiviert ist.
3. Aktualisieren Sie das System, das als Host für den ePolicy Orchestrator-Server dienen soll, und den SQL-Server mit den aktuellen Microsoft-Sicherheits-Updates, und deaktivieren Sie dann Windows-Updates für die Dauer der Installation.

4. Überzeugen Sie sich, dass die vom primären Server kopierte SQL-Sicherungsdatei nach dem Microsoft-SQL-Prozess wiederhergestellt wurde.
5. Beenden Sie vor der Wiederherstellung von ePolicy Orchestrator auf allen Systemen die remoten Agentensteuerungsdienste.



Bei einer Installation vom Typ **Wiederherstellen** müssen Sie den gesamten Installationsvorgang überwachen. Möglicherweise müssen Sie das System neu starten.

Vorgehensweise

1. Wenn Sie remote Agentensteuerungen konfiguriert haben, melden Sie sich bei den Systemen an, auf denen die Agentensteuerungen installiert sind. Öffnen Sie dann das Windows-Fenster **Dienste**, und beenden Sie die Dienste **McAfee-Ereignisanalyse** und **McAfee-Apache**.

   Weitere Informationen zur Verwendung des Windows-Fensters **Dienste** finden Sie in der Produktdokumentation von Microsoft.

2. Melden Sie sich mit einem Konto, das über lokale Administratorrechte verfügt, bei dem Windows-Computer an, der als ePolicy Orchestrator-Wiederherstellungs-Server dient.
3. Extrahieren Sie die Dateien, die Sie von der McAfee-Website heruntergeladen haben, in einen temporären Speicherort, und doppelklicken Sie dann auf die Datei `SETUP.EXE`.

   Versuchen Sie nicht, die Datei `SETUP.EXE` auszuführen, bevor Sie den Inhalt der ZIP-Datei extrahiert haben.

   Der **McAfee ePolicy Orchestrator – InstallShield-Assistent** wird gestartet.

4. Klicken Sie auf **ePO aus einem vorhandenen Datenbank-Snapshot wiederherstellen** und auf **Weiter**, um mit der Wiederherstellungsinstallation zu beginnen.
5. Im Schritt **Zusätzliche Software installieren** sind alle noch erforderlichen Komponenten aufgelistet. Klicken Sie für deren Installation auf **Weiter**.

   Wenn SQL Express installiert wird, ist Microsoft .NET Framework 2.0 (oder höher) erforderlich. Diese Software wird nicht automatisch installiert. Wenn diese Software fehlt, müssen Sie das Setup beenden und die Software manuell installieren, bevor Sie fortfahren können.

6. Klicken Sie im Schritt **Zielordner** auf Folgendes:
   - **Weiter** – Installieren Sie McAfee ePO im Standardspeicherort (`C:\Programme\McAfee\ePolicy Orchestrator (x86)\`).
   - **Ändern** – Geben Sie einen benutzerdefinierten Zielspeicherort für McAfee ePO an. Wenn das Fenster **Aktuellen Zielordner ändern** geöffnet wird, wechseln Sie zum Zielordner, und erstellen Sie gegebenenfalls neue Ordner. Klicken Sie abschließend auf **OK**.
7. Wählen Sie im Schritt **Datenbankinformationen** den Namen des Microsoft SQL-Servers in der Liste **Datenbank-Server** aus, und geben Sie an, welcher Typ von **Anmeldeinformationen für Datenbank-Server** verwendet werden soll. Klicken Sie anschließend auf **Weiter**.

Windows-Authentifizierung	1 Wählen Sie im Menü **Domäne** die Domäne des Benutzerkontos aus, das Sie zum Zugreifen auf den SQL-Server verwenden möchten. 2 Geben Sie **Benutzername** und **Kennwort** Ihrer wiederhergestellten SQL-Datenbank ein.
SQL-Authentifizierung	• Geben Sie **Benutzername** und **Kennwort** für Ihren SQL-Server ein. Vergewissern Sie sich, dass die von Ihnen angegebenen Anmeldeinformationen einem im SQL-Server vorhandenen Benutzer mit entsprechenden Berechtigungen gehören. Bei Verwendung von SQL-Authentifizierung ist das Menü **Domäne** ausgegraut.



Möglicherweise müssen Sie den **TCP-Port für SQL-Server** eingeben, über den die Kommunikation zwischen Ihrem McAfee ePO-Server und dem Datenbank-Server erfolgen soll. Die ePolicy Orchestrator-Installation versucht, über die Standardports (1433 und 1434) eine Verbindung herzustellen. Falls dies nicht möglich ist, werden Sie zur Eingabe eines TCP-Ports für den SQL-Server aufgefordert.

8 Überprüfen Sie im Schritt **HTTP-Portinformationen** die standardmäßig zugewiesenen Ports. Klicken Sie auf **Weiter**, um zu überprüfen, dass diese Ports auf dem System nicht bereits belegt sind.



Einige dieser Ports können Sie jetzt ändern. Weitere Informationen über das Ändern von Portnummern finden Sie unter How to change the ePO 4.5.0 and 4.6.0 Agent-to-Server communication port (Vorgehensweise zum Ändern des Ports für die Agent-zu-Server-Kommunikation in ePO 4.5.0 und 4.6.0).

9 Geben Sie im Schritt **Administratorinformationen** den **Benutzernamen** und das **Kennwort** ein, die Sie beim Administratorkonto des zuvor vorhandenen Servers verwendet haben.

10 Geben Sie die **Passphrase für die Schlüsselspeicherverschlüsselung** ein, die Sie während der Erstinstallation des vorherigen McAfee ePO-Servers verwendet oder in den **Server-Einstellungen** geändert haben.

Mit der Passphrase für die Schlüsselspeicherverschlüsselung werden die vertraulichen Dateien im Snapshot für die Wiederherstellung nach einem Systemausfall entschlüsselt.

11 Geben Sie im Schritt **Lizenzschlüssel eingeben** Ihren Lizenzschlüssel ein, und klicken Sie dann auf **Weiter**.

Wenn Sie keinen Lizenzschlüssel besitzen, können Sie die Option **Test** auswählen, um mit der Installation der Software fortzufahren. Die Testphase ist auf 90 Tage begrenzt. Nach Abschluss der Installation können Sie einen Lizenzschlüssel innerhalb der Anwendung eingeben. Weitere Informationen hierzu finden Sie im *Produkthandbuch von ePolicy Orchestrator* oder in der Hilfe.

12 Erklären Sie sich mit dem **McAfee Endbenutzer-Lizenzvertrag** einverstanden, und klicken Sie auf **OK**.

13 Legen Sie im Dialogfeld **Bereit zum Installieren des Programms** fest, ob Sie anonyme Nutzungsinformationen an McAfee senden möchten, und klicken Sie dann auf **Installieren**, um mit der Installation der Software zu beginnen.



Wenn McAfee keine anonymen Diagnose- und Nutzungsdaten erfassen soll, deaktivieren Sie das Kontrollkästchen.

14 Klicken Sie nach Abschluss der Installation auf **Fertig stellen**, um den InstallShield-Assistenten zu beenden.



Dieses Dialogfeld enthält Kontrollkästchen, die Sie aktivieren können, wenn Sie nach Abschluss der Installation die Versionsinformationen lesen möchten oder ePolicy Orchestrator gestartet werden soll.

15 Wenn Sie ePolicy Orchestrator auf einem McAfee ePO-Server wiederhergestellt haben, der eine andere IP-Adresse oder einen anderen DNS-Namen als der vorherige Server hat, müssen Sie eine Möglichkeit konfigurieren, über die Ihre verwalteten Systeme eine Verbindung zu dem neuen McAfee ePO-Server herstellen können.



Am besten erstellen Sie dazu einen CNAME-Eintrag im DNS, der Anfragen, die an die alte Adresse (IP-Adresse, DNS-Name oder NetBIOS-Name) des vorherigen McAfee ePO-Servers gerichtet sind, auf die neuen Informationen des McAfee ePO-Wiederherstellungs-Servers verweist.

16 Wenn Sie die remoten Agentensteuerungen in Schritt 1 beendet haben, melden Sie sich bei den Systemen an, auf denen die Agentensteuerungen installiert sind. Öffnen Sie dann das Windows-Fenster **Dienste**, und starten Sie die Dienste **McAfee-Ereignisanalyse** und **McAfee-Apache**.

ePolicy Orchestrator ist nun wiederhergestellt. Falls erforderlich, doppelklicken Sie auf Ihrem Desktop auf das Schildsymbol, um mit Ihrem McAfee ePO-Server zu arbeiten, oder wechseln Sie auf einer remoten Web-Konsole zu dem Server (`https://<Server-Name>:<Port>`).



Wenn Sie mit remoten Agentensteuerungen arbeiten, finden Sie unter *Wiederherstellen der Verbindung bei remoten Agentensteuerungen* Informationen darüber, wie Sie deren Einstellungen ändern, damit sie eine Verbindung zu den wiederhergestellten Servern herstellen können.

Wiederherstellen von ePolicy Orchestrator in einer Cluster-Umgebung

Wenn Sie die auf Server-Clustern mit MSCS (Microsoft Cluster Server) installierten McAfee ePO-Server wiederherstellen möchten, müssen Sie ePolicy Orchestrator auf sämtlichen Servern in dem Cluster neu installieren.

Bevor Sie beginnen

Lesen, verstehen und befolgen Sie unbedingt die im Kapitel *Anforderungen und Empfehlungen für die Installation* aufgeführten Punkte.

Wenn Sie den vorhandenen SQL-Server auswählen, müssen Sie vor Beginn der Installation die folgenden Informationen sammeln und die folgenden Schritte durchführen, um sicherzustellen, dass McAfee ePO mit dem Datenbank-Server kommunizieren kann:

1 Stellen Sie sicher, dass der **SQL Browser-Dienst** ausgeführt wird.

2 Stellen Sie sicher, dass im SQL Server-Konfigurations-Manager das TCP/IP-Protokoll aktiviert ist.

3 Aktualisieren Sie das System, das als Host für den ePolicy Orchestrator-Server dienen soll, und den SQL-Server mit den aktuellen Microsoft-Sicherheits-Updates, und deaktivieren Sie dann Windows-Updates für die Dauer der Installation.

4 Überzeugen Sie sich, dass die vom primären Server kopierte SQL-Sicherungsdatei nach dem Microsoft-SQL-Prozess wiederhergestellt wurde.

5 Beenden Sie vor der Wiederherstellung von ePolicy Orchestrator auf allen Systemen die remoten Agentensteuerungsdienste.



Bei einer Installation vom Typ **Wiederherstellen** müssen Sie den gesamten Installationsvorgang überwachen. Möglicherweise müssen Sie das System neu starten.

Die Wiederherstellung von ePolicy Orchestrator in einer MSCS-Umgebung ähnelt der Erstinstallation der Software. Der einzige Unterschied sind die Anweisungen in Schritt 6.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wenn Sie remote Agentensteuerungen konfiguriert haben, melden Sie sich bei den Systemen an, auf denen die Agentensteuerungen installiert sind. Öffnen Sie dann das Windows-Fenster **Dienste**, und beenden Sie die Dienste **McAfee-Ereignisanalyse** und **McAfee-Apache**.



Weitere Informationen zur Verwendung des Windows-Fensters **Dienste** finden Sie in der Produktdokumentation von Microsoft.

2. Führen Sie die Cluster-Installation durch. Unter *Durchführen einer Cluster-Installation* erhalten Sie einen Überblick über den Ablauf einer Cluster-Software-Installation.
3. Installieren Sie ePolicy Orchestrator unter Windows Server 2008 oder Windows Server 2012. Unter *Installieren auf einem System mit Windows Server 2008 oder Windows Server 2012* finden Sie eine Liste mit den Schritten zur Erstinstallation der Software.
4. Erstellen Sie die Anwendungsgruppe "ePolicy Orchestrator". Unter *Erstellen der ePolicy Orchestrator-Anwendungsgruppe* sind die Schritte aufgeführt, die zur Trennung der ePolicy Orchestrator-Anwendung von den Microsoft Cluster-Diensten in einer Cluster-Umgebung durchgeführt werden müssen.
5. Erstellen Sie den Client-Zugriffspunkt. Unter *Erstellen des Client-Zugriffspunkts* wird beschrieben, wie Sie eine virtuelle IP-Adresse und virtuelle Netzwerknamen für ePolicy Orchestrator definieren, damit Ihre Cluster-Knoten mit Ihrem McAfee ePO-Server kommunizieren können.
6. Fügen Sie das Datenlaufwerk hinzu. Unter *Hinzufügen des Datenlaufwerks* wird beschrieben, wie Sie den Pfad zu dem Datenlaufwerk festlegen, auf dem Sie ePolicy Orchestrator installieren.
7. Stellen Sie ePolicy Orchestrator auf den einzelnen Knoten wie nachfolgend beschrieben wieder her.



Führen Sie die **Cluster**-Installation auf jedem Knoten des Clusters aus. Damit sichergestellt ist, dass jeder Knoten während der Installation über exklusiven Zugriff auf die Quorum- und Datenlaufwerke verfügt, müssen Sie alle anderen Knoten im Cluster herunterfahren.

   a. Melden Sie sich mit einem Konto, das über lokale Administratorrechte verfügt, bei dem Windows-Computer an, der als ePolicy Orchestrator-Wiederherstellungs-Server dient.
   b. Führen Sie das Setup-Programm aus der Software aus, die Sie von der McAfee-Website heruntergeladen haben, extrahieren Sie die Dateien in einen temporären Speicherort, und doppelklicken Sie auf **SETUP.EXE**.



Versuchen Sie nicht, die Datei `SETUP.EXE` auszuführen, bevor Sie die ZIP-Datei extrahiert haben.

   Der **McAfee ePolicy Orchestrator – InstallShield-Assistent** wird gestartet.
   c. Klicken Sie auf **ePO aus einem vorhandenen Datenbank-Snapshot wiederherstellen** und auf **Weiter**, um mit der Wiederherstellungsinstallation zu beginnen.
   d. Folgen Sie den Anweisungen des Assistenten, bis Sie zur Seite **Setup-Typ** gelangen. Wählen Sie dort die Option **Cluster** aus, und klicken Sie dann auf **Weiter**.
   e. Geben Sie auf der Seite **Zielverzeichnis auswählen** den Pfad für das freigegebene Datenlaufwerk ein, und klicken Sie dann auf **Weiter**.

   Verwenden Sie für jeden Knoten denselben Pfad.

f Geben Sie auf der Seite **Einstellungen für virtuellen Server festlegen** (nur auf dem ersten Knoten) die folgenden Identifizierungsinformationen für den McAfee ePO-Cluster an:

- Die IP-Adresse des virtuellen ePolicy Orchestrator-Servers
- Den Namen des virtuellen ePolicy Orchestrator-Clusters
- Den vollqualifizierten Domänennamen (FQDN) des virtuellen ePolicy Orchestrator-Clusters



Diese Informationen werden automatisch auf nachfolgenden Knoten bereitgestellt.

g Führen Sie die Installation auf dem ersten Knoten wie unter *Durchführen einer benutzerdefinierten Installation* beschrieben durch.

h Wiederholen Sie diese Schritte für jeden Knoten im Cluster.

8. Aktivieren Sie die Ressourcen "Allgemeiner Dienst" für den Cluster-Server. Unter *Erstellen der Ressourcen "Allgemeiner Dienst"* wird beschrieben, wie der McAfee ePO-Server durch Starten und Anhalten der ePolicy Orchestrator-Dienste gesteuert wird.
9. Wenn Sie die remoten Agentensteuerungen in Schritt 1 beendet haben, melden Sie sich bei den Systemen an, auf denen die Agentensteuerungen installiert sind. Öffnen Sie dann das Windows-Fenster **Dienste**, und starten Sie die Dienste **McAfee-Ereignisanalyse** und **McAfee-Apache**.
10. Stellen Sie sicher, dass die Software bei einem Failover funktioniert. Weitere Informationen dazu finden Sie unter *Testen der ePolicy Orchestrator-Cluster-Installation*.

Nach Abschluss dieser Schritte ist ePolicy Orchestrator auf allen Servern im Server-Cluster wiederhergestellt.

Wiederherstellen der Verbindung bei remoten Agentensteuerungen

Nachdem Sie den McAfee ePO-Server und die SQL-Datenbank wiederhergestellt haben, müssen Sie die Einstellungen der remoten Agentensteuerungen ändern, damit diese eine Verbindung zu den wiederhergestellten Servern herstellen können.

Bevor Sie beginnen

Aktualisieren Sie das System mit den aktuellen Microsoft-Sicherheits-Updates, und deaktivieren Sie dann Windows-Updates für die Dauer der Installation.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Suchen Sie auf dem Server-System mit der Agentensteuerung den Ordner `Agent Handler`, den Sie aus dem ePolicy Orchestrator-Installationspaket extrahiert haben.
2. Doppelklicken Sie auf `SETUP.EXE`, um den McAfee-InstallShield-Assistenten für Agentensteuerungen zu starten. Nach einigen Installationsaktivitäten im Hintergrund wird der InstallShield-Assistent gestartet. Klicken Sie auf **Weiter**, um mit der Änderung zu beginnen.
3. Klicken Sie im Dialogfeld **Programmwartung** auf **Ändern**, um festzulegen, welche Programmfunktionen installiert werden sollen.

   Die Seite mit den Server-Informationen wird geöffnet.

4 Konfigurieren Sie die folgenden Einstellungen:

a Geben Sie den Computernamen des wiederhergestellten McAfee ePO-Servers ein, mit dem die Agentensteuerung kommunizieren soll.

b Geben Sie den Port an, über den die Kommunikation von der Agentensteuerung zum Server erfolgen soll. Der Standardport ist 8444 – der gleiche wie der **Port für authentifizierte Client-zu-Server-Kommunikation**.



Bei Verwendung des Standardports kann die Kommunikation von der Agentensteuerung zum Server über einen einzigen Port (8444) erfolgen. Optional können Sie auch den Port 8443 (**Konsolen-Port zur Anwendungs-Server-Kommunikation**) angeben. In diesem Fall muss aber der Port 8444 weiterhin für die Agentensteuerungs-Kommunikation verfügbar sein.

c Geben Sie als ePO-Administratorinformationen den **Benutzernamen** und das **Kennwort** eines Benutzers mit globalen Administratorrechten für ePolicy Orchestrator ein.

d Klicken Sie auf **Weiter**, damit die **ePO-Administrator**-Anmeldeinformationen auch für den Zugriff auf die Datenbank verwendet werden. Stellen Sie dabei sicher, dass diesen die entsprechende SQL Server-Rolle und die entsprechenden SQL Server-Berechtigungen zugewiesen sind.

e Deaktivieren Sie **Anmeldeinformationen für ePO-Server-Datenbank verwenden**, und klicken Sie dann auf **Weiter**.

Die Seite mit den **Datenbankinformationen** wird geöffnet.

5 Konfigurieren Sie die neuen Anmeldeinformationen für den Zugriff auf die wiederhergestellte Datenbank, und klicken Sie anschließend auf **Weiter**:

- **Datenbank-Server** mit Instanzname. Zum Beispiel: `DB-SERVER\SERVER-NAME`.
- Authentifizierungstyp.
- Name der **Domäne**, in der sich der wiederhergestellte Datenbank-Server befindet.
- **Benutzername** und **Kennwort**.
- **Datenbankname** (sofern nicht automatisch angegeben).

6 Klicken Sie auf **Installieren**, um mit der Änderung der Installation zu beginnen. Nach Abschluss der Installation müssen Sie die remote Agentensteuerung auf der Benutzeroberfläche von ePolicy Orchestrator aktivieren. Weitere Informationen zum Aktivieren einer remoten Agentensteuerung finden Sie unter *Arbeiten mit Agentensteuerungen* im Produkthandbuch oder in der Hilfe.

Die remoten Agentensteuerungen können nun mit dem wiederhergestellten McAfee ePO-Server und der SQL-Datenbank kommunizieren.

4 Aktualisieren von ePolicy Orchestrator

Sie können *bestimmte* Versionen der Software ePolicy Orchestrator 4.5 und 4.6 auf die Version 5.0 aktualisieren. Ausführliche Informationen dazu finden Sie unter *Mindestversionen für ein Upgrade von ePolicy Orchestrator.*

Inhalt

Vorbereiten auf eine Aktualisierung

Damit ein Upgrade erfolgreich verläuft, müssen Sie Ihre Umgebung vorbereiten und sicherstellen, dass Sie über eine Mindestversion von ePolicy Orchestrator verfügen. Lesen Sie sich die folgenden Informationen sorgfältig durch, bevor Sie mit dem Upgrade beginnen.

Sie müssen die folgenden Schritte durchführen:

- Überprüfen Sie die Liste der nicht unterstützten Produkte.
- Sichern Sie alle ePolicy Orchestrator-Datenbanken.
- Sichern Sie das gesamte ePolicy Orchestrator-Verzeichnis.
- Deaktivieren Sie alle remoten Agentensteuerungen in der Umgebung.
- Deaktivieren Sie Windows-Updates, bevor Sie mit der Aktualisierung beginnen.
- Lesen, verstehen und befolgen Sie unbedingt die im Kapitel *Anforderungen und Empfehlungen für die Installation* aufgeführten Punkte, bevor Sie mit dem Upgrade beginnen.



Anders als bei früheren Versionen muss die Version 5.0 von ePolicy Orchestrator auf einer 64-Bit-Plattform installiert sein.

Mindestversionen für ein Upgrade von ePolicy Orchestrator

Nur die folgenden Versionen von ePolicy Orchestrator können auf ePolicy Orchestrator 5.0 aktualisiert werden:

- ePolicy Orchestrator 4.5 Patch 6 oder höher
- ePolicy Orchestrator 4.6 Patch 4 oder höher

Unterstützte und nicht unterstützte Produkte

Vor einer Installation oder Aktualisierung sollten Sie die Liste der von ePolicy Orchestrator unterstützten Produkte durchsehen.

Eine aktualisierte Liste mit unterstützten bzw. nicht unterstützten Produkten finden Sie in den folgenden KnowledgeBase-Artikeln:

- Von McAfee ePO 5.0 unterstützte Produkte – KB76736 (https://kc.mcafee.com/corporate/index?page=content&id=KB76736)
- Von McAfee ePO 5.0 nicht unterstützte Produkte – KB76737 (https://kc.mcafee.com/corporate/index?page=content&id=KB76737)
- Prüfliste mit bekannten Problemen bei der McAfee ePO 5.0-Installation bzw. dem Upgrade mithilfe eines Patches – KB76739 (https://kc.mcafee.com/corporate/index?page=content&id=KB76739)

Sichern der ePolicy Orchestrator-Datenbanken und -Verzeichnisse

Vor dem Aktualisieren der Software müssen Sie alle ePolicy Orchestrator-Datenbanken sowie das ePolicy Orchestrator-Verzeichnis sichern.

Ausführliche Informationen dazu finden Sie im KnowledgeBase-Artikel für ePolicy Orchestrator 4.5 und 4.6 – KB66616 (https://kc.mcafee.com/corporate/index?page=content&id=KB66616)

Deaktivieren von remoten Agentensteuerungen vor dem Aktualisieren

Wenn Sie eine Aktualisierung von ePolicy Orchestrator 4.X aus durchführen und in der Umgebung remote Agentensteuerungen verwendet werden, müssen Sie diese deaktivieren, damit die Aktualisierung fehlerfrei durchgeführt werden kann.

Wenn die remoten Agentensteuerung deaktiviert sind, können Sie den Server aktualisieren. Nach Abschluss der Aktualisierung müssen Sie auch die Agentensteuerungen aktualisieren. Weitere Informationen dazu finden Sie unter *Aktualisieren remoter Agentensteuerungen*.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Öffnen Sie die Seite **Steuerungsliste**. Klicken Sie dazu in der Benutzeroberfläche von ePolicy Orchestrator auf **Menü** | **Konfiguration** | **Agentensteuerungen** und dann im Monitor **Steuerungsstatus** auf **Agentensteuerungen**.



2. Klicken Sie auf der Seite **Steuerungsliste** bei jeder remoten Agentensteuerung, die Sie installiert haben, auf **Deaktivieren.**
3. Melden Sie sich bei dem System an, auf dem die Agentensteuerung installiert ist, öffnen Sie dann das Windows-Fenster **Dienste**, und beenden Sie die Dienste **McAfee-Ereignisanalyse** und **McAfee-Apache.**



Weitere Informationen zur Verwendung des Windows-Fensters **Dienste** finden Sie in der Dokumentation des Microsoft-Produkts.

Überblick über das Upgrade-Kompatibilitätsprogramm

Wenn Sie ein Upgrade einer vorhandener Installation von ePolicy Orchestrator 4.X auf eine ePolicy Orchestrator-Plattform der Version 5.0 durchführen, müssen Sie dieses Dienstprogramm ausführen, um Ihre bestehende Konfiguration auf den Upgrade-Server zu kopieren und eine Produktkompatibilitätsüberprüfung durchzuführen.

Das Upgrade-Kompatibilitätsprogramm führt folgende Aufgaben durch:

- Es konvertiert die vorhandene McAfee ePO 4.X-Konfiguration aus der vorhandenen Plattform, und kopiert sie auf die neue Plattform der Version 5.0.
- Es stellt mithilfe einer Produktkompatibilitätsüberprüfung fest, ob eine der installierten McAfee ePO 4.X-Erweiterungen *nicht* mit der neuen Upgrade-Version von ePolicy Orchestrator kompatibel ist.

Produktkompatibilitätsüberprüfung

Eine erste Produktkompatibilitätsliste ist bereits im ePolicy Orchestrator-Paket enthalten, das Sie von der McAfee-Website heruntergeladen haben. Bei der Produktkompatibilitätsüberprüfung lädt das Programm eine aktuelle Liste der kompatiblen Erweiterungen von einer vertrauenswürdigen McAfee-Quelle über das Internet herunter. Wenn die Internetquelle nicht verfügbar ist oder wenn die heruntergeladene Liste nicht verifiziert werden kann, verwendet ePolicy Orchestrator die letzte gespeicherte Version.

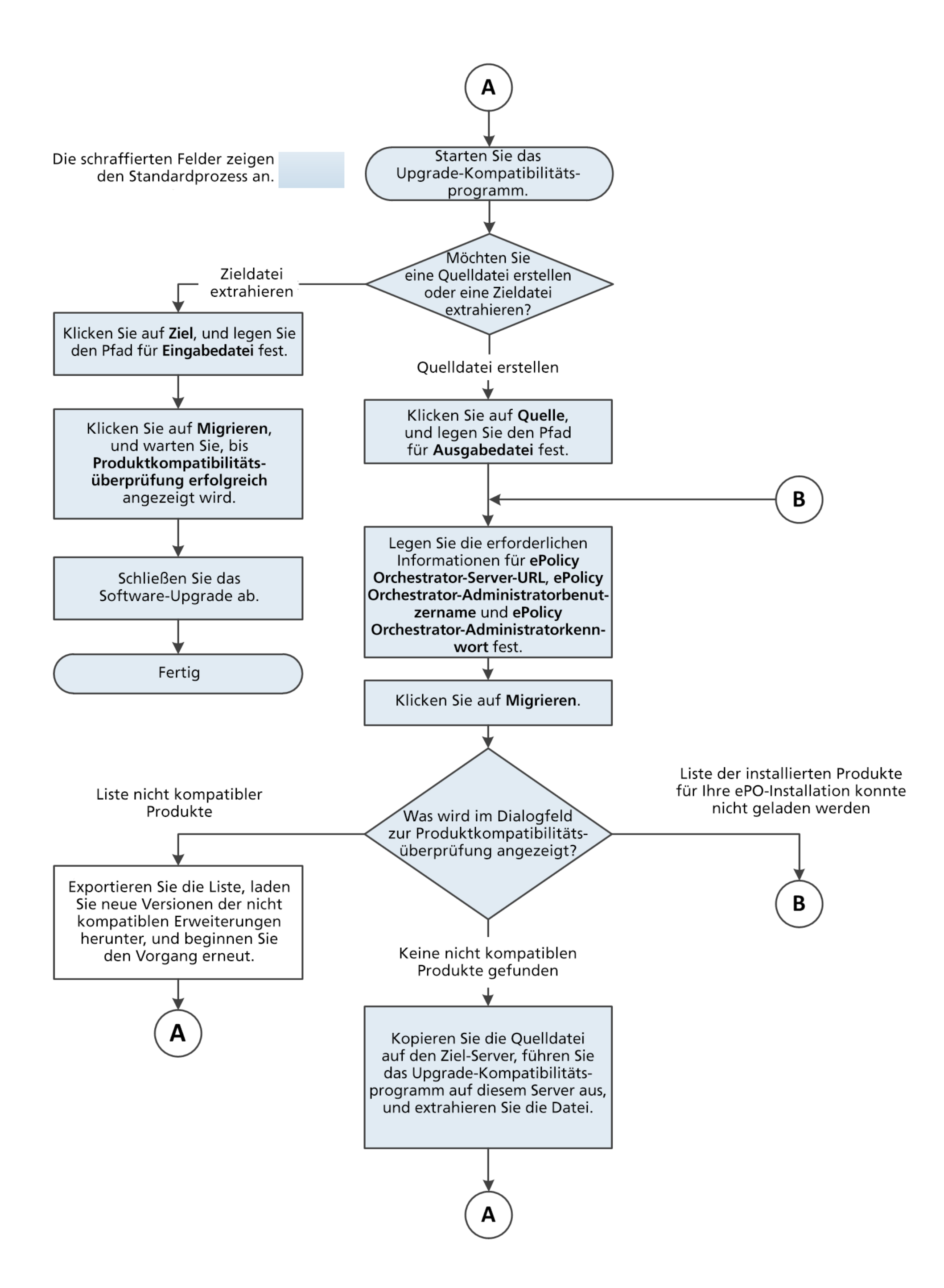


Sofern Sie in den **Server-Einstellungen** die Option **Produktkompatibilitätsliste** aktiviert haben, wird diese Liste vom McAfee ePO-Server einmal täglich im Hintergrund aktualisiert.

Die Produktkompatibilitätsüberprüfung stellt entweder fest, dass die aktuellen Produkterweiterungen mit der neuen Version von ePolicy Orchestrator kompatibel sind, oder sie erstellt eine Liste der blockierten oder deaktivierten Erweiterungen.

- **Blockierte** Erweiterungen verhindern ein Upgrade der ePolicy Orchestrator-Software.
- **Deaktivierte** Erweiterungen verhindern das Upgrade nicht, sie werden jedoch nach dem ePolicy Orchestrator-Upgrade erst dann initialisiert, wenn eine bekannte Ersatzerweiterung installiert wurde.

Die für den Upgrade-Kompatibilitätsprozess erforderlichen Schritte sind im folgenden Ablaufdiagramm beschrieben.


Die schraffierten Felder zeigen den Standardprozess an.
A
Starten Sie das Upgrade-Kompatibilitäts-programm.
Möchten Sie eine Quelldatei erstellen oder eine Zieldatei extrahieren?
Zieldatei extrahieren
Klicken Sie auf Ziel, und legen Sie den Pfad für Eingabedatei fest.
Klicken Sie auf Migrieren, und warten Sie, bis Produktkompatibilitäts-überprüfung erfolgreich angezeigt wird.
Schließen Sie das Software-Upgrade ab.
Fertig
Quelldatei erstellen
Klicken Sie auf Quelle, und legen Sie den Pfad für Ausgabedatei fest.
B
Legen Sie die erforderlichen Informationen für ePolicy Orchestrator-Server-URL, ePolicy Orchestrator-Administratorbenut-zername und ePolicy Orchestrator-Administratorkenn-wort fest.
Klicken Sie auf Migrieren.
Was wird im Dialogfeld zur Produktkompatibilitäts-überprüfung angezeigt?
Liste nicht kompatibler Produkte
Exportieren Sie die Liste, laden Sie neue Versionen der nicht kompatiblen Erweiterungen herunter, und beginnen Sie den Vorgang erneut.
A
Liste der installierten Produkte für Ihre ePO-Installation konnte nicht geladen werden
B
Keine nicht kompatiblen Produkte gefunden
Kopieren Sie die Quelldatei auf den Ziel-Server, führen Sie das Upgrade-Kompatibilitäts-programm auf diesem Server aus, und extrahieren Sie die Datei.
A

Ausführen des Dienstprogramms

Mit diesem Programm können Sie eine vorhandene ePolicy Orchestrator 4.X-Konfiguration in eine neue Konfigurationsdatei für die Version 5.0 (oder höher) konvertieren.

Bevor Sie beginnen

1. Sichern Sie Ihre ePolicy Orchestrator-Datenbank, bevor Sie das Upgrade-Kompatibilitätsprogramm von ePolicy Orchestrator ausführen.
2. Extrahieren Sie die Installations-Software für ePolicy Orchestrator 5.0, und wechseln Sie in den Ordner **UpgradeCompatibility**. In diesem Ordner befindet sich die Datei `UPGRADECOMPATIBILITY.EXE`.
3. Für den Einsatz des Upgrade-Kompatibilitätsprogramms ist Microsoft .NET Framework 3.5 (oder höher) erforderlich. Informationen über den Download und die Installation dieses Frameworks erhalten Sie im Microsoft Download Center.



Wenn Sie versuchen, das Programm ohne installiertes Framework auszuführen, wird ein Fehler angezeigt.

Das Dienstprogramm führt auch eine Produktkompatibilitätsüberprüfung durch, um festzustellen, ob vorhandene Produkterweiterungen eine erfolgreiche Migration von Version 4.X auf 5.0 (oder höher) verhindern könnten.



Dieses Dienstprogramm wurde speziell für die Konvertierung von 32-Bit-Konfigurationen von McAfee ePO 4.X in 64-Bit-Konfigurationen der Version 5.0 (oder höher) entworfen.

Vorgehensweise

1. Suchen Sie das **ePolicy Orchestrator-Upgrade-Kompatibilitätsprogramm**, und führen Sie es aus.
   a. Laden Sie die Software für ePolicy Orchestrator 5.0 von der McAfee-Website herunter.
      Die Software befindet sich in der heruntergeladenen ePolicy Orchestrator-Installationsdatei.
   b. Extrahieren Sie die Dateien in einen temporären Speicherort, wechseln Sie in den Ordner `UpgradeCompatibility`, und doppelklicken Sie auf die Datei **UPGRADECOMPATIBILITY.EXE**.
      Das **ePolicy Orchestrator-Upgrade-Kompatibilitätsprogramm** wird angezeigt.
2. Erstellen Sie die Ausgabedatei der Quelle für die Version 4.X.
   a. Klicken Sie unter **Server-Typ** auf **Quelle**.
   b. Klicken Sie auf **Ausgabedatei**, wechseln Sie in das Verzeichnis, in dem Sie die ePolicy Orchestrator-Datendatei speichern möchten, und fügen Sie einen Namen mit der Erweiterung `.ZIP` hinzu. In der Standardeinstellung wird die Datei unter **C:\MIGRATE.ZIP** gespeichert.
   c. Geben Sie die folgenden Informationen für die Remote-Anmeldung bei Ihrem vorhandenen McAfee ePO-Server an:
      - **ePolicy Orchestrator-Server-URL**
      - **ePolicy Orchestrator-Administratorbenutzername**
      - **ePolicy Orchestrator-Administratorkennwort**

d Wählen Sie aus, welche Datei der Produktkompatibilitätsliste verwendet werden soll:

- Wenn **Produktkompatibilitätsliste automatisch abrufen** aktiviert ist – Bei der Produktkompatibilitätsüberprüfung wird automatisch die aktuellste Liste von einer vertrauenswürdigen McAfee-Quelle über das Internet abgerufen. Wenn die Internetquelle nicht verfügbar ist oder die Liste nicht verifiziert werden kann, wird die Liste verwendet, die zusammen mit der aktuellen ePolicy Orchestrator-Version heruntergeladen wurde.
- Wenn **Produktkompatibilitätsliste automatisch abrufen** deaktiviert ist — Bei der Produktkompatibilitätsüberprüfung wird die Produktkompatibilitätsliste verwendet, die manuell heruntergeladen wurde.



Klicken Sie auf PRODUCTCOMPATIBILITYLIST.XML, um die Datei manuell herunterzuladen.

e Klicken Sie auf **Migrieren** oder **Produktkompatibilitätsüberprüfung.** Im Dialogfeld zur Produktkompatibilitätsüberprüfung für ePO wird eine der folgenden Meldungen angezeigt:

- **Keine nicht kompatiblen Produkte gefunden** – Sie können mit Schritt 3 fortfahren.

  Der Komprimierungsvorgang kann auf einem ePolicy Orchestrator-Unternehmens-Server mehrere Minuten in Anspruch nehmen.
- **Liste nicht kompatibler Produkte** – Hierbei handelt es sich um eine Liste der blockierten und deaktivierten Erweiterungen. Ersetzen Sie die in dieser Liste aufgeführten blockierten Erweiterungen durch Versionen, die mit dieser Version der Software kompatibel sind, und führen Sie dann die Produktkompatibilitätsüberprüfung erneut durch.

  Wenn eine Erweiterung deaktiviert ist, wird das Upgrade dadurch nicht blockiert, die Erweiterung wird nach Abschluss des ePolicy Orchestrator-Upgrades jedoch erst aktiviert, wenn eine bekannte Ersatzerweiterung installiert wurde.
- **Liste der installierten Produkte für Ihre ePO-Installation konnte nicht geladen werden** – Das bedeutet, dass die Datei mit der Produktkompatibilitätsliste nicht verfügbar ist, oder dass die von Ihnen eingegebenen Informationen für den Zugriff auf den McAfee ePO-Quell-Server fehlerhaft waren. Kehren Sie zu Schritt 2c zurück, und wiederholen Sie den Vorgang.



Falls Sie die Erstellung der Migrationsdatei unterbrechen müssen, beginnen Sie einfach noch einmal von vorn, um eine neue Datei zu erstellen.

Status zeigt den Verlauf der Dateierstellung an, und bei Abschluss des Vorgangs wird die Meldung **Migration abgeschlossen** angezeigt.

3 Auf dem Upgrade-Server:

a Laden Sie die Software für ePolicy Orchestrator 5.0 von der McAfee-Website herunter.

Die Software befindet sich in der heruntergeladenen ePolicy Orchestrator-Installationsdatei.



Sie können die Software für ePolicy Orchestrator 5.0 auch von Ihrem vorhandenen McAfee ePO 4.X-Server kopieren, auf den Sie sie heruntergeladen haben.

b Extrahieren Sie die Dateien in einen temporären Speicherort, wechseln Sie in den Ordner `UpgradeCompatibility`, und doppelklicken Sie auf die Datei **UPGRADECOMPATIBILITY.EXE.**

Das ePolicy Orchestrator-Upgrade-Kompatibilitätsprogramm wird angezeigt.

c Kopieren Sie die ePolicy Orchestrator-Datendatei, die Sie erstellt haben, auf den Upgrade-Server.



Wenn Sie McAfee® VirusScan® Enterprise auf dem Upgrade-Server installiert haben, müssen Sie den On-Access-Scan deaktivieren, bevor Sie die 4.X-Dateien auf den 5.0-Server kopieren.

d Klicken Sie unter **Server-Typ** auf **Ziel.**

e Klicken Sie auf **Eingabedatei**, und wechseln Sie zu dem Speicherort, in den Sie die Quellkonfigurationsdatei vom 4.X-Quell-Server kopiert haben. In der Standardeinstellung wird die Datei unter `C:\MIGRATE.ZIP` gespeichert.

f Klicken Sie auf **Migrieren**, um die ePolicy Orchestrator-Konfigurationsdateien der Version 4.X zu extrahieren und in Konfigurationsdateien für die Version 5.0 (oder höher) zu konvertieren.

Status zeigt den Verlauf der Dateiextrahierung an, und bei Abschluss des Vorgangs wird die Meldung **Migration abgeschlossen** angezeigt. Der Extrahierungsvorgang kann auf einem McAfee ePO-Unternehmens-Server mehrere Minuten in Anspruch nehmen.



Falls Sie die Extrahierung der Migrationsdatei unterbrechen müssen, starten Sie einfach den ePolicy Orchestrator 5.0-Upgrade-Server neu, und beginnen Sie den Migrationsvorgang noch einmal von vorn, um die Datei zu extrahieren.

4 Führen Sie das im Abschnitt *Aktualisieren von McAfee ePolicy Orchestrator* beschriebene Upgrade durch.

Alle vorhandenen Konfigurationsdateien des McAfee ePO 4.X-Servers wurden auf den McAfee ePO-Server der Version 5.0 (oder höher) kopiert. Nun können Sie das Upgrade für ePolicy Orchestrator ausführen.



Falls das Upgrade von ePolicy Orchestrator fehlschlägt und Sie eine Migration ausgeführt haben und dann das Upgrade auf ePolicy Orchestrator 5.0 durchführen, müssen Sie zu Ihrer Sicherungsdatenbank auf dem 4.X-Server zurückkehren.

Aktualisieren des ePolicy Orchestrator-Servers

Mithilfe der Datei `SETUP.EXE` können Sie einen ePolicy Orchestrator 4.X-Server auf die Version 5.0 aktualisieren.

Bevor Sie beginnen

Aktualisieren Sie das System, das als Host für den ePolicy Orchestrator-Server dient, mit den aktuellen Microsoft-Sicherheits-Updates, und deaktivieren Sie dann Windows-Updates für die Dauer der Installation.

Unter *Vorbereiten auf eine Aktualisierung* sind die Mindestversionen für ein Upgrade von ePolicy Orchestrator aufgeführt.



Es wird empfohlen, den Aktualisierungsvorgang zu überwachen. Möglicherweise müssen Sie das System neu starten.

Der Standardspeicherort von ePolicy Orchestrator lautet: `C:\Programme (x86)\McAfee\ePolicy Orchestrator`

Vorgehensweise

1 Melden Sie sich bei dem System mit einem Konto an, das über lokale Administratorrechte verfügt.

2 Laden Sie auf dem zu aktualisierenden McAfee ePO 5.0-Server (64-Bit) die Software für ePolicy Orchestrator 5.0 von der McAfee-Website herunter.

Die Software befindet sich in der heruntergeladenen ePolicy Orchestrator-Installationsdatei.

3. Entpacken Sie die Dateien in einen temporären Speicherort, und doppelklicken Sie auf `SETUP.EXE`.



Wenn auf dem Zielcomputer der Installation erforderliche Software fehlt, wird eine entsprechende Liste angezeigt. Klicken Sie auf **Weiter**. Der Installationsvorgang wird für jedes aufgeführte Software-Element automatisch gestartet.

4. Klicken Sie auf der Seite **Willkommen** des Installations-Assistenten auf **Weiter**.

   Möglicherweise wird eine Warnmeldung mit einer Liste der Produkte aus der früheren Version von ePolicy Orchestrator angezeigt, die in Version 5.0 nicht mehr unterstützt werden. Diese Produkte werden nicht in das ePolicy Orchestrator 5.0-Repository migriert.

5. Geben Sie im Dialogfeld mit den **Informationen zum globalen Administrator** den Benutzernamen und das Kennwort des globalen Administrators für den aktuellen Server ein, und klicken Sie dann auf **Weiter**.

6. Legen Sie im Dialogfeld **Bereit zum Installieren des Programms** fest, ob Sie **Anonyme Nutzungsinformationen an McAfee senden** möchten, und klicken Sie dann auf **Installieren**, um mit der Installation der Software zu beginnen.



Wenn McAfee keine anonymen Diagnose- und Nutzungsdaten erfassen soll, deaktivieren Sie das Kontrollkästchen.

7. Klicken Sie im Dialogfeld **InstallShield-Assistent abgeschlossen** auf **Fertig stellen**, um die Installation abzuschließen.

Aktualisieren des ePolicy Orchestrator-Cluster-Servers

Beim Aktualisieren der ePolicy Orchestrator-Software in einer Cluster-Umgebung müssen einige besondere Aspekte berücksichtigt werden.

Bevor Sie beginnen

Wenn Sie auf die Version 5.0 von ePolicy Orchestrator aktualisieren und Ihre aktuelle Umgebung von dieser Version nicht unterstützt wird, müssen Sie vor dem Aktualisieren von ePolicy Orchestrator die erforderlichen Schritte zum Aktualisieren der Umgebung durchführen.

Sie können einen ePolicy Orchestrator-Cluster-Server von bestimmten 4.5- und 4.6-Versionen auf die Version 5.0 aktualisieren. Unter *Vorbereiten auf eine Aktualisierung* sind die Mindestversionen für ein Upgrade von ePolicy Orchestrator aufgeführt.

Vorgehensweise

1. Öffnen Sie auf dem aktiven Knoten die **ePO-Gruppe** in der **Windows-Clusterverwaltung** (2008: Failover-Clusterverwaltung). Schalten Sie jede der folgenden Ressourcen vom Typ "Allgemeiner Dienst" offline, und löschen Sie sie dann:
   - McAfee ePolicy Orchestrator 4.x.x-Server
   - McAfee ePolicy Orchestrator 4.x.x-Anwendungs-Server
   - McAfee ePolicy Orchestrator 4.x.x-Ereignisanalyse

Die folgenden Ressourcen, die für ein erfolgreiches Upgrade erforderlich sind, dürfen Sie nicht ändern:

- Das Datenlaufwerk
- Die virtuelle IP-Adresse von ePolicy Orchestrator
- Den virtuellen Netzwerknamen von ePolicy Orchestrator

2 Öffnen Sie den **Dienststeuerungs-Manager**, und stellen Sie sicher, dass die folgenden Dienste ausgeführt werden:

- McAfee ePolicy Orchestrator 4.x.x-Server
- McAfee ePolicy Orchestrator 4.x.x-Anwendungs-Server
- McAfee ePolicy Orchestrator 4.x.x-Ereignisanalyse

Wiederholen Sie diesen Schritt auf jedem Knoten, bevor Sie mit der Installation der neuen Software beginnen.

3 Installieren Sie Ihre neue ePolicy Orchestrator-Software auf jedem Knoten.



Bei einem Upgrade von Version 4.5 aus müssen Sie die Reihenfolge beachten, in der Sie die Version 4.5 auf den einzelnen Knoten installiert haben. Beginnen Sie mit dem Upgrade auf dem gleichen Knoten wie bei der ursprünglichen Installation. Wenn Sie zum Beispiel die Version 4.5 von ePolicy Orchestrator auf den Knoten A, B und C (in dieser Reihenfolge) installiert haben, müssen Sie zuerst den Knoten A aktualisieren. In welcher Reihenfolge Sie nachfolgende Knoten aktualisieren, spielt keine Rolle.

Eine ausführliche Installationsanleitung finden Sie im Kapitel *Installieren von ePolicy Orchestrator auf jedem Knoten* unter *Durchführen einer Cluster-Installation*.

4 Nach Abschluss der Installation auf den einzelnen Knoten erstellen Sie die neuen Ressourcen vom Typ "Allgemeiner Dienst" für die Version 5.0 der Software. Wie diese Ressourcen konfiguriert werden, hängt vom Betriebssystem ab. Ausführliche Informationen zur Konfiguration unter den einzelnen Betriebssystemen finden Sie im Abschnitt *Erstellen der Ressourcen "Allgemeiner Dienst"* unter *Durchführen einer Cluster-Installation*.

Aktualisieren remoter Agentensteuerungen

Beim Aktualisieren der Software auf dem ePolicy Orchestrator-Server müssen Sie auch alle in der Umgebung installierten remoten Agentensteuerungen aktualisieren. Agentensteuerungen müssen separat aktualisiert werden.

Remote Agentensteuerungen, die mit älteren Versionen Ihrer Software installiert wurden, sind mit dieser neuen Version nicht kompatibel und werden nicht automatisch aktualisiert.

Der Aktualisierungsvorgang ist ein vereinfachter Ablauf der Erstinstallation einer remoten Agentensteuerung, die in *Installieren remoter Agentensteuerungen* unter *Installieren von McAfee ePolicy Orchestrator* näher beschrieben wird.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Kopieren Sie den Ordner `Agent Handler` aus dem Installationspaket der ePolicy Orchestrator-Software auf das Zielsystem.

2 Doppelklicken Sie auf **SETUP.EXE**, um den McAfee-InstallShield-Assistenten für Agentensteuerungen zu starten.

3. Klicken Sie auf **Weiter**, um mit der Aktualisierung zu beginnen.
4. Akzeptieren Sie den Lizenzvertrag, und klicken Sie dann auf **OK**.
5. Klicken Sie auf **Installieren**, um mit der Installation zu beginnen.
6. Der InstallShield-Assistent führt die Installation durch, ohne dass weitere Eingaben erforderlich sind. Klicken Sie abschließend auf **Fertig stellen**.
7. Nach Abschluss der Aktualisierung müssen Sie die remote Agentensteuerung auf der Benutzeroberfläche von ePolicy Orchestrator aktivieren.

   Weitere Informationen zum Aktivieren einer remoten Agentensteuerung finden Sie unter *Arbeiten mit Agentensteuerungen* im *Produkthandbuch* oder in der Hilfe.

5 Deinstallieren von ePolicy Orchestrator

Unter Umständen müssen Sie ePolicy Orchestrator deinstallieren, z. B. wenn Sie die Software auf einem anderen Server neu installieren möchten. In den folgenden Themen wird beschrieben, wie Sie eine Deinstallation durchführen.



Wenn Sie ePolicy Orchestrator zu einem späteren Zeitpunkt wieder installieren und von der aktuellen Installation ausgebrachte Agenten verwalten möchten, müssen Sie Ihre Schlüssel für die Agenten-Server-Kommunikation sichern. Diese Schlüssel können Sie später nicht wiederherstellen.

Inhalt

Deinstallieren von Express- und benutzerdefinierten Installationen

Beim Deinstallieren von Express- und benutzerdefinierten Installationen der ePolicy Orchestrator-Software müssen bestimmte Punkte hinsichtlich der Datenbank beachtet werden.



Wenn Sie SQL Server 2008 Express mithilfe des Setup-Programms installiert haben, können Sie die zu diesem SQL-Server hinzugefügte Datenbank beim Deinstallieren von ePolicy Orchestrator mit entfernen.

Vorgehensweise

1. Schließen Sie sämtliche Datenbankverwaltungs-Software.
2. Öffnen Sie auf dem System, auf dem der ePolicy Orchestrator-Server installiert ist, die Windows-**Systemsteuerung**, und klicken Sie dann auf **Programme und Funktionen** | **McAfee ePolicy Orchestrator** | **Deinstallieren/Ändern**.
3. Das Dialogfeld **McAfee ePolicy Orchestrator entfernen** wird angezeigt. Wählen Sie aus, ob Sie die **ePolicy Orchestrator-Datenbank ebenfalls entfernen** möchten, und klicken Sie dann auf **Entfernen**.



Geben Sie Anmeldeinformationen an, die über entsprechende Berechtigungen verfügen, um die Datenbank entfernen zu können. Wenn die angegebenen Anmeldeinformationen nicht über ausreichende Berechtigungen verfügen, können Sie festlegen, dass die Deinstallation ohne Entfernen der Datenbank durchgeführt werden soll. Weitere Informationen zu SQL Server-Berechtigungen finden Sie unter *Warten der ePolicy Orchestrator-Datenbanken* im Produkthandbuch oder in der Hilfe.

Deinstallieren von Cluster-Installationen

Beim Deinstallieren von ePolicy Orchestrator in einer Cluster-Umgebung müssen je nach dem Server-Betriebssystem, auf dem die Software ausgeführt wird, bestimmte Schritte durchgeführt werden.

Vorgehensweise

1. Öffnen Sie zum Umschalten aller McAfee ePO-Dienste in den Offline-Modus die **Windows-Clusterverwaltung**, und klicken Sie dann auf **Start | Programme | Verwaltung | Failover-Clusterverwaltung**.
2. Klicken Sie in der McAfee ePO-Anwendungsgruppe mit der rechten Maustaste auf jede der McAfee ePO-Ressourcen, und wählen Sie **Löschen** aus.
3. Klicken Sie zum Deinstallieren der Software auf **Programme und Funktionen | McAfee ePolicy Orchestrator | Deinstallieren/Ändern**.
4. Wiederholen Sie diese Schritte auf jedem Knoten im Cluster.

6 Referenzmaterial zu Fehlerbehebung und Protokolldateien

In diesem Kapitel sind die Meldungen, die während einer Installation von McAfee ePolicy Orchestrator am häufigsten angezeigt werden, mit den zugehörigen Lösungen aufgelistet. Nutzen Sie die nachfolgend aufgeführten Informationen, um Probleme bei Ihrer Installation zu beheben.

Wenn Sie ein Problem nicht mithilfe der in dieser Tabelle aufgeführten Informationen beheben können, wenden Sie sich an den technischen Support von McAfee. Führen Sie jedoch zuvor die folgenden Schritte durch:

1. Stellen Sie sicher, dass die Mindestanforderungen für die Installation erfüllt werden.
2. Lesen Sie in den *Versionsinformationen zu McAfee ePolicy Orchestrator 5.0* (`README.HTML`) den Abschnitt über die bekannten Installationsprobleme.
3. Stellen Sie sicher, dass das Benutzerkonto, mit dem Sie sich bei dem Computer angemeldet haben, auf dem Sie die Software installieren, über vollständige Administratorrechte für diesen Computer verfügt.
4. Notieren Sie sich den genauen Wortlaut jeder einzelnen Nachricht und von jedem angezeigten Nachrichten-Code.
5. Stellen Sie die Installationsprotokolldateien zusammen.

Inhalt

Häufige Installationsmeldungen sowie deren Ursachen und Lösungen

ePolicy Orchestrator gibt während des Installationsvorgangs Rückmeldungen aus, die möglicherweise zusätzliche Aktionen erfordern. In der folgenden Tabelle finden Sie weitere Informationen zu Aktionen, die bei solchen Meldungen durchzuführen sind.

Meldung	Ursache	Lösung
Sie versuchen, eine Produktversion zu aktualisieren, die nicht unterstützt wird. Eine vollständige Liste der Anforderungen für eine Aktualisierung finden Sie im *Installationshandbuch von McAfee ePolicy Orchestrator*.	Auf diesem Computer wurde keine Version von ePolicy Orchestrator installiert. Sie können nur ein Upgrade der *ePolicy Orchestrator-Mindestversionen* durchführen, die unter *Vorbereiten auf eine Aktualisierung* aufgeführt sind.	Lesen Sie dazu *Installieren von McAfee ePolicy Orchestrator* in diesem Handbuch, und wählen Sie eine geeignete Installationsoption aus.
Internet Explorer 8.0 (oder höher) oder Firefox 10 muss installiert sein, damit diese Installation fortgesetzt werden kann.	Der Computer, auf dem die Software installiert werden soll, verwendet eine nicht unterstützte Version des Browsers.	Installieren Sie einen unterstützten Internetbrowser, bevor Sie den Vorgang fortsetzen. Weitere Informationen dazu finden Sie unter *Unterstützte Internet-Browser*.
Es wird bereits eine andere Instanz des Installationsprogramms für McAfee ePolicy Orchestrator ausgeführt.	Das Setup-Programm für ePolicy Orchestrator 5.0 wird bereits ausgeführt. Es kann jeweils nur eine Instanz des Installationsprogramms ausgeführt werden.	Warten Sie, bis die erste Instanz des Installationsprogramms die Installation abgeschlossen hat, oder beenden Sie die erste Instanz, und starten Sie Ihre Installation erneut.
Aus Sicherheitsgründen müssen Kennwörter ausgefüllt werden. Geben Sie ein gültiges Kennwort ein, um fortzufahren.	Das Feld **Kennwort** ist leer.	Geben Sie ein Kennwort für das Benutzerkonto ein, das Sie verwenden möchten.
McAfee empfiehlt, die Auflösung der Grafikanzeige auf mindestens 1024x768 einzustellen.	Der Computer, auf dem die Software installiert werden soll, erfüllt nicht die Mindestanforderung für die Bildschirmauflösung.	Ändern Sie die Bildschirmauflösung auf mindestens 1024 x 768, und setzen Sie anschließend die Installation fort. Andernfalls können Sie nach dem Starten der Software möglicherweise nicht den gesamten Bildschirm sehen. Anweisungen zum Ändern der Bildschirmauflösung finden Sie in der Windows-Hilfedatei. Klicken Sie dazu auf **Start**, und wählen Sie dann **Hilfe** aus.
McAfee empfiehlt, die Software auf einem Computer mit mindestens 2 GB RAM zu installieren.	Der Computer, auf dem die Software installiert werden soll, erfüllt nicht die Mindestanforderung für den Arbeitsspeicher.	Erhöhen Sie den Speicher des Systems, oder wählen Sie für die Installation ein anderes System aus, das über mindestens 2 GB RAM verfügt.

Meldung	Ursache	Lösung
Damit ePolicy Orchestrator 5.0 ausgeführt werden kann, muss auf Ihrem Computer Windows Server 2008 oder Windows Server 2012 ausgeführt werden.	Der Computer, auf dem die Software installiert werden soll, verwendet eine nicht unterstützte Version des Betriebssystems.	Siehe dazu *Unterstützte Server-Betriebssysteme*.
Geben Sie einen Wert in das Feld 'Kommunikationsport für Agenten-Übertragung' ein.	Das Feld **Kommunikationsport für Agenten-Übertragung** ist leer.	Geben Sie die Nummer des Ports an (standardmäßig 8082), den der ePolicy Orchestrator-Server zum Senden von Agenten-Reaktivierungen an SuperAgents verwenden soll.
Geben Sie einen Wert in das Feld 'Port für Agent-zu-Server-Kommunikation' ein.	Das Feld **Port für Agent-zu-Server-Kommunikation** ist leer.	Geben Sie die Nummer des Ports an, den der Agent zum Kommunizieren mit dem Server verwenden soll.
Geben Sie einen Wert in das Feld 'Kommunikationsport für Agenten-Reaktivierung' ein.	Das Feld **Kommunikationsport für Agenten-Reaktivierung** ist leer.	Geben Sie die Nummer des Ports an (standardmäßig 8081), den der ePolicy Orchestrator-Server zum Senden von Agenten-Reaktivierungen verwenden soll.
ePolicy Orchestrator muss in einen Ordner installiert werden. Geben Sie einen Zielordner ein, um fortzufahren.	Das Feld **Zielordner** ist leer oder gibt das Stammverzeichnis eines Laufwerks an.	Klicken Sie auf **Durchsuchen**, um einen Speicherort auszuwählen. Der Standardspeicherort ist: `C:\Programme\McAfee\ePolicy Orchestrator`.
Geben Sie einen Wert in das Feld 'Benutzername' ein.	Das Feld **Benutzername** ist leer.	Geben Sie den Benutzernamen des Kontos an, das Sie verwenden möchten.
Die Lizenzdatei ist nicht vorhanden oder beschädigt. Wenden Sie sich an den Support, wenn Sie Hilfe benötigen.	Die für die Installation der Software erforderlichen Lizenzinformationen können nicht gelesen werden.	Wenden Sie sich an den technischen Support von McAfee.
Das von Ihnen verwendete Betriebssystem oder Service Pack wird derzeit nicht unterstützt. Eine Auflistung der Systemanforderungen finden Sie im *Installationshandbuch von McAfee ePolicy Orchestrator*.	Der Computer, auf dem die Software installiert werden soll, verwendet eine nicht unterstützte Version des Betriebssystems.	Siehe dazu *Unterstützte Server-Betriebssysteme*.
Die eingegebenen Kennwörter stimmen nicht überein. Geben Sie ein gültiges Kennwort ein, um fortzufahren.	Die Werte, die Sie in die Felder **Kennwort** und **Kennwort bestätigen** eingegeben haben, stimmen nicht überein.	Geben Sie das Kennwort für das Konto ein, das Sie verwenden möchten.
Die ePolicy Orchestrator-Lizenz ist abgelaufen.	Ihre Lizenz zur Nutzung der Software ist abgelaufen.	Wenden Sie sich an Ihren Administrator oder den zuständigen McAfee-Mitarbeiter.

Meldung	Ursache	Lösung
Dieses System ist derzeit nicht mit einer statischen IP-Adresse konfiguriert. Für den ePolicy Orchestrator-Server wird eine statische IP-Adresse empfohlen.	Der Computer, auf dem die Software installiert werden soll, verwendet keine statische IP-Adresse. Es wird empfohlen, statische IP-Adressen für ePolicy Orchestrator-Server zu verwenden, um die Leistung zu verbessern und die Bandbreitenauslastung zu reduzieren.	Geben Sie eine statische IP-Adresse an, die Ihr ePolicy Orchestrator-Server verwenden soll.
Die Verbindung zum Datenbank-Server kann nicht hergestellt werden. Überprüfen Sie, ob Sie die Anmeldeinformationen für das Konto und den Namen des Datenbank-Servers richtig eingegeben haben, und versuchen Sie es erneut. Wenn diese Meldung weiterhin angezeigt wird, finden Sie im *Installationshandbuch von ePolicy Orchestrator* weitere Informationen.	Die Verbindung zum entsprechenden ePolicy Orchestrator-Datenbank-Server konnte nicht hergestellt werden.	1 Überprüfen Sie, ob die **Domäne**, der **Benutzername** und das **Kennwort** korrekt eingegeben wurden. 2 Stellen Sie sicher, dass der Datenbank-Server ausgeführt wird. 3 Stellen Sie sicher, dass das eingegebene Benutzerkonto für diesen Datenbank-Server gültig ist.
Mit den von Ihnen angegebenen Informationen kann keine Verbindung hergestellt werden. Überprüfen Sie, ob Sie die richtigen Informationen eingegeben haben, und versuchen Sie es erneut.	Auf das von Ihnen angegebene Benutzerkonto kann nicht zugegriffen werden.	1 Überprüfen Sie, ob die **Domäne**, der **Benutzername** und das **Kennwort** korrekt eingegeben wurden. 2 Stellen Sie sicher, dass das Konto, mit dem Sie sich bei diesem Computer angemeldet haben, über Zugriffsberechtigung für diese Domäne verfügt.

Protokolldateien für die Fehlerbehebung

ePolicy Orchestrator verfügt über Protokolldateien, die wichtige Informationen für die Fehlerbehebung enthalten.

Diese Protokolldateien sind in drei Kategorien eingeteilt:

- **Installationsprotokolle** – Enthalten Details über den Installationspfad, die Benutzeranmeldeinformationen, die verwendete Datenbank und die konfigurierten Kommunikationsports.
- **Server-Protokolle** – Enthalten Details über die Server-Funktionen, den Verlauf von Client-Ereignissen und die Administratordienste.
- **Agenten-Protokolle** – Enthalten Details über die Agenten-Installationen, Reaktivierungen, Aktualisierungen und Richtlinienerzwingungen.

Installationsprotokolle

Installationsprotokolldateien geben Details über den Installationsvorgang von ePolicy Orchestrator an.

Dazu gehören Informationen über:

- Von bestimmten Komponenten durchgeführte Aktionen
- Vom Server genutzte Administratordienste
- Erfolg oder Fehlfunktion wichtiger Vorgänge

Dateiname	Protokolltyp	Speicherort	Beschreibung
AH500-INSTALL-MSI.LOG	Agentensteuerungs-Installation	%temp%\McAfeeLogs	In dieser Datei werden alle Details zu Installationen von Agentensteuerungen protokolliert. Dazu gehören: • Aktionen des Installationsprogramms • Installationsfehler
AH500-AHETUPDLL.LOG	Temporär	%temp% (auf dem Agentensteuerungs-Server)	Protokolliert Agentensteuerungs-Backend-Ereignisse.
CORE-INSTALL.LOG	Temporär	%tmp%\McAfeeLogs\ePO500-Troubleshoot\MFS	Wird generiert, wenn das Installationsprogramm von ePolicy Orchestrator das MFS ANT-Installationsprogramm aufruft. Es enthält Informationen über: • Erstellung von Server-Datenbanktabellen • Installation von Server-Komponenten Bei einer erfolgreichen Installation wird diese Datei gelöscht.
EPO-INSTALL.LOG	Installation	%tmp%\McAfeeLogs\ePO500-Troubleshoot\Mercury Framework	Wird erstellt, wenn das Installationsprogramm von ePolicy Orchestrator das ANT-Installationsprogramm aufruft.
EPO500-CHECKIN-FAILURE.LOG	Installation	%temp%\McAfeeLogs	Wird generiert, wenn ein Paket eines der folgenden Typen nicht vom Installationsprogramm von ePolicy Orchestrator eingecheckt werden kann: • Erweiterungen • Plug-Ins • Ausbringungspakete • Agenten-Pakete

Dateiname	Protokolltyp	Speicherort	Beschreibung
`EPO500-COMMONSETUP.LOG`	Installation	`%temp%\McAfeeLogs`	Enthält Details zum Installationsprogramm von ePolicy Orchestrator. Dazu gehören: • Protokollierung von benutzerdefinierten Aktionen • Aufrufe von SQL, DTS (Microsoft Data Transformation Services) und zugehöriger Dienste • Registrierung und Aufhebung der Registrierung von DLLs • Ausgewählte Dateien und Ordner, die nach dem Neustart gelöscht werden sollen
`EPO500-INSTALL-MSI.LOG`	Installation	`%temp%\McAfeeLogs`	Das primäre Installationsprotokoll von ePolicy Orchestrator. Es enthält Installationsdetails, z. B. vom Installationsprogramm durchgeführte Aktionen und Installationsfehler.
`<Erweiterungsdateiname>.CMD`	Temporär	`%temp%\McAfeeLogs\ePO500-troubleshoot\OutputFiles`	Wird vom ePolicy Orchestrator-Installationsprogramm erstellt. Es enthält den (an den Remote-Client gesendeten) Befehl zum Einchecken von Erweiterungen. Bei einer erfolgreichen Installation werden diese Dateien gelöscht.
`MFS500-COMMONSETUP.LOG`	Installation	`%tmp%\McAfeeLogs`	Enthält Details zum MFS-Installationsprogramm.

Server-Protokolle

Server-Protokolldateien enthalten Details zu Server-Funktionen und verschiedenen Administratordiensten, die von ePolicy Orchestrator genutzt werden.

Dateiname	Protokolltyp	Speicherort	Beschreibung
`EPOAPSVR.LOG`	Primär	`[INSTALLATIONSVERZEICHNIS]\DB\Logs`	Protokolldatei des Anwendungs-Servers mit Details zu Repository-Aktionen. Dazu gehören: • Abruf-Tasks • Einchecken von Ausbringungspaketen in das Repository • Löschen von Ausbringungspaketen im Repository Diese Datei ist erst nach dem ersten Dienststart vorhanden.
`ERRORLOG.<AKTUELLES DATUM UND AKTUELLE UHRZEIT>`	Apache	`[INSTALLATIONSVERZEICHNIS]\Apache2\logs`	Enthält Details zum Apache-Dienst. Diese Datei ist erst nach dem ersten Starten des Apache-Diensts vorhanden.

Dateiname	Protokolltyp	Speicherort	Beschreibung
EVENTPARSER .LOG	Primär	[INSTALLATIONSVERZEICHNIS] \DB\Logs	Enthält Details über die ePolicy Orchestrator-Ereignisanalysedienste, wie zum Beispiel erfolgreiche oder fehlgeschlagene Produktereignisanalysen.
JAKARTA _SERVICE _<DATUM>.LOG	Tomcat	[INSTALLATIONSVERZEICHNIS] \Server\logs *	Enthält Details zum ePolicy Orchestrator-Anwendungs-Server-Dienst. Diese Datei ist erst nach dem ersten Start des Tomcat-Diensts vorhanden.
LOCALHOST _ACCESS_LOG .<DATUM>.TXT	Tomcat	[INSTALLATIONSVERZEICHNIS] \Server\logs *	Enthält alle von Client-Systemen beim McAfee ePO-Server eingegangenen Anfragen. Diese Datei ist erst nach dem ersten Start des Tomcat-Diensts vorhanden.
ORION.LOG	Primär	[INSTALLATIONSVERZEICHNIS] \Server\logs *	Enthält Details zur McAfee Foundation Services-Plattform sowie alle standardmäßig geladenen Erweiterungen. Diese Datei ist erst nach dem ersten Starten des ePolicy Orchestrator-Anwendungs-Server-Diensts vorhanden.
REPLICATION .LOG	Server	[INSTALLATIONSVERZEICHNIS] \DB\Logs	Die Protokolldatei für die McAfee ePO-Server-Replizierung. Diese Datei wird nur dann generiert, wenn alle folgenden Bedingungen erfüllt sind: • Es sind verteilte Repositories vorhanden. • Es wurde ein Replizierungs-Task konfiguriert. • Es wurde ein Replizierungs-Task ausgeführt.
SERVER.LOG	Primär	[INSTALLATIONSVERZEICHNIS] \DB\Logs	Enthält Details zu den folgenden McAfee ePO-Server-Diensten: • Agent-zu-Server-Kommunikationen • Agentensteuerung des McAfee ePO-Servers Diese Datei ist erst nach dem ersten Dienststart vorhanden.
STDERR.LOG	Tomcat	[INSTALLATIONSVERZEICHNIS] \Server\logs *	Enthält alle vom Tomcat-Dienst erfassten Ausgaben von Standardfehlern. Diese Datei ist erst nach dem ersten Start des Tomcat-Diensts vorhanden.

* In Cluster-Umgebungen befindet sich das Protokoll unter [INSTALLATIONSVERZEICHNIS]\Bin\Server\logs.

Agenten-Protokolle

Agenten-Protokolldateien enthalten Aktionen, die von McAfee® Agent ausgelöst oder durchgeführt wurden.

Dateiname	Protokolltyp	Speicherort	Beschreibung
<AGENTEN-GUID>_<ZEITSTEMPEL>_SERVER.XML	Richtlinie	[INSTALLATIONSVERZEICHNIS]\DB\DEBUG	Enthält Details über Probleme bei der Richtlinienaktualisierung. Gehen Sie zum Aktivieren dieser Datei folgendermaßen vor: 1 Wechseln Sie zu dem folgenden Registrierungsschlüssel: HKEY_LOCAL_MACHINE\Software\Network Associates\ePolicy Orchestrator\ 2 Erstellen Sie den folgenden DWORD mit dem Wert 1: SaveAgentPolicy 3 Starten Sie den McAfee ePolicy Orchestrator 5.0.0-Server-(Apache-)Dienst neu. Sie sollten diese Datei nur für die Mindestzeitdauer aktivieren, die für die Erfassung der erforderlichen Informationen benötigt wird, da die resultierenden Dateien schnell an Größe zunehmen.
AGENT_<SYSTEM>.LOG	Agent	[PFAD ZU AGENTEN-DATEN]\DB	Wird auf Client-Systemen generiert, wenn der Server auf ihnen einen Agenten ausbringt. Diese Datei enthält Details über: • Agent-zu-Server-Kommunikation • Richtlinienerzwingung • Andere Agenten-Tasks
FRMINST_<SYSTEM>.LOG	Agent	%temp%\McAfeeLogs	Wird generiert, wenn McAfee Agent mithilfe der Datei FRMINST.EXE installiert wird. Die Datei enthält Folgendes: • Meldungen mit informativem Charakter • Meldungen zum Fortschritt • Fehlermeldungen (falls eine Installation fehlschlägt)
MCSCRIPT.LOG	Agent-Debug	[PFAD ZU AGENTEN-DATEN]\DB	Enthält die Ergebnisse von Skriptbefehlen, die bei einer Ausbringung oder Aktualisierung von Agenten verwendet werden. Wenn Sie für dieses Protokoll den DEBUG-Modus aktivieren möchten, legen Sie im Registrierungsschlüssel des Clients den folgenden DWORD-Wert fest: HKEY_LOCAL_MACHINE\SOFTWARE\NETWORK ASSOCIATES\TVD\SHARED COMPONENTS\FRAMEWORK\DWDEBUGSCRIPT=2 Löschen Sie den Schlüssel nach Abschluss der Fehlerbehebung wieder.
MFEAGENT.MSI.<DATUM>.LOG	Agent	%temp%\McAfeeLogs	Enthält Details über die MSI-Installation des Agenten.

Dateiname	Protokolltyp	Speicherort	Beschreibung
PRDMGR _<SYSTEM>.LOG	Agent	[PFAD ZU AGENTEN-DATEN]\DB	Enthält Details über die Kommunikation des Agenten mit anderen McAfee-Produkten.
UPDATERUI _<SYSTEM>.LOG	Agent	%temp%\McAfeeLogs	Enthält Details über Aktualisierungen an verwalteten Produkten auf dem Client-System.

McAfee Agent-Fehlerprotokolle

Wenn McAfee Agent Fehler feststellt, werden diese in Agenten-Fehlerprotokollen erfasst. Diese Agenten-Fehlerprotokolle sind nach dem Gegenstück ihres jeweiligen primären Protokolls benannt. Wenn beispielsweise beim Ausführen von Client-Tasks Fehler auftreten, wird die Datei MCSCRIPT_ERROR .LOG erstellt. Fehlerprotokolle enthalten nur Details über Fehler.

Index


McAfee
An Intel Company